

*Via Electronic Filing*

December 23, 2019

Marlene H. Dortch, Esq.  
Secretary  
Federal Communications Commission  
445 Twelfth St., SW  
Washington, DC 20554

**Re: Authorization of Radiofrequency Equipment, ET Docket No. 15-170**

Dear Ms. Dortch:

On December 19, 2019, we met with Umair Javed, Legal Advisor to Commissioner Jessica Rosenworcel, to discuss the primary initiatives of the Council to Secure the Digital Economy (CSDE), namely the development of and follow-up on three CSDE reports: *International Botnet and IoT Security Guide 2020*; *Cyber Crisis: Foundations of Multi-Stakeholder Coordination*; and *The C2 Consensus on IoT Device Security Baseline Capabilities*. We were accompanied in the meeting by Mike Bergman of CTA, Paul Eisler of USTelecom, and our outside counsel, Clete Johnson and Erik Jones of Wilkinson Barker Knauer, LLP.

We provided Mr. Javed an overview of how these CSDE activities advance government-industry partnership and meaningful improvements in cybersecurity in coordination with the Sector Coordinating Councils for the Communications and IT Sectors; the Information and Communication Technology Supply Chain Risk Management Task Force; the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and National Risk Management Center (NRMC); the Commerce Department's National Telecommunications and Information Administration (NTIA) and National Institute for Standards and Technology (NIST); and the FCC. The discussion focused in particular on IoT security and the role that the C2 Consensus is playing in driving IoT security standards and retailer requirements, touching briefly on general equipment authorization issues pertinent to the above-referenced docket.

Sincerely,

/s/ Jamie Susskind

Jamie Susskind  
Vice President, Policy and Regulatory Affairs  
Consumer Technology Association

/s/ Mike Saperstein

Mike Saperstein  
Vice President, Policy and Advocacy  
USTelecom – The Broadband Association

cc: Umair Javed

Enclosure



Council to Secure the  
Digital Economy

# INTERNATIONAL BOTNET AND IOT SECURITY GUIDE 2020



## NOTICE

The International Botnet and IoT Security Guide was developed to facilitate the mitigation of botnets and other automated, distributed threats through voluntary participation and collaboration among disparate stakeholders throughout the global internet and communications ecosystem. The Guide provides information and encouragement to Information and Communications Technology (ICT) stakeholders about affirmative measures to implement towards this goal as they deem appropriate, based upon their individual circumstances and their relationships with each other.

The Guide highlights impactful voluntary practices for each segment of the ICT sector, ranging from “baseline” to “advanced.” While the industry leaders who have developed this Guide recognize that no combination of measures can guarantee the elimination of all threats and risks, they believe these practices, both baseline and advanced, present a valuable framework for ICT stakeholders to reference in identifying and choosing practices of their own to mitigate the threats of automated, distributed attacks. The Guide recognizes that different ICT stakeholders face different challenges, considerations, and priorities as they implement security measures. Accordingly, the practices identified in this Guide, and the Guide as a whole, are tools that ICT stakeholders should implement according to their circumstances; they are not requirements or mandates, or otherwise compulsory in any way.

Many of the practices and technologies discussed in this document are already being used by large-scale enterprises to protect their networks and systems, ranging from contracting for deep packet inspection (DPI) from network service providers to prohibiting the use of devices that do not have sufficient built-in security measures. However, the implementation of these capabilities in the wider consumer space has broader policy implications. For example:

Advanced capabilities such as DPI of IP traffic, while useful in certain contexts, could have significant implications for individual privacy if deployed on public networks.

- ▶ If required by governments to meet other policy objectives, filtering of public network traffic based on IP addresses and other means may also have implications for the free flow of information.
- ▶ Enterprises have skilled IT staff who negotiate detailed requirements with their suppliers and incorporate cost-benefit analyses in decisionmaking. Such dynamics do not exist in the consumer space, where the cost-benefit analysis can differ significantly from that of a large-scale enterprise. For consumers, cost and consumer protection issues will need to be evaluated on a different risk management scale.
- ▶ Devices that are deemed to have insufficient security capabilities cannot simply be banned from sale in a given country on an ad hoc basis without considering international trade implications and other local regulations.

---

### COPYRIGHT STATEMENT

*Copyright © 2019 by USTelecom® and the Consumer Technology Association (CTA)™. All rights reserved. This document may not be reproduced, in whole or part, without written permission. Federal copyright law prohibits unauthorized reproduction of this document by any means. Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. Requests to reproduce text, data, charts, figures or other material should be made to [copyright@securingdigitaleconomy.org](mailto:copyright@securingdigitaleconomy.org).*

# Contents

<b>01</b>	Executive Summary.....	1
<b>02</b>	Introduction.....	6
<b>03</b>	The Evolution of Botnets: Year in Review.....	9
<b>04</b>	Addressing Automated, Distributed Threats in a Diverse Internet Ecosystem ....	17
<b>05</b>	Practices and Capabilities of Components of the Ecosystem.....	19
	A. <i>Infrastructure</i> .....	19
	1. Detect Malicious Traffic and Vulnerabilities.....	21
	2. Mitigate Against Distributed Threats.....	23
	3. Coordinate with Customers and Peers.....	27
	4. Address Domain Seizure and Takedown.....	21
	B. <i>Software Development</i> .....	28
	1. Secure-by-Design Development Practices.....	28
	2. Security Vulnerability Management.....	30
	3. Transparency of Secure Development Processes .....	30
	C. <i>IoT Devices</i> .....	30
	1. Secure Development.....	31
	2. Secure Capabilities.....	31
	3. Product Lifecycle Management .....	36
	D. <i>Home and Small Business Systems Installation</i> .....	37
	1. Authentication and Credential Management.....	37
	2. Network Configuration .....	37
	3. Network Hardware Management.....	38
	4. Security Maintenance .....	40
	E. <i>Enterprises</i> .....	40
	1. Secure Updates.....	41
	2. Real-time Information Sharing.....	41
	3. Network Architectures that Securely Manage Traffic Flows .....	42
	4. Enhanced DDoS Resilience .....	43
	5. Identity and Access Management .....	44
	6. Mitigating Issues with Out-of-Date and Pirated Products.....	46
<b>06</b>	Next Steps and Conclusion .....	47
<b>07</b>	Contributing Organizations.....	48
<b>08</b>	Endnotes.....	49





## 01/ Executive Summary

Since the release last year of the *International Anti-Botnet Guide 2018* by the CSDE, industry has continued to step up efforts to push back on distributed attacks. However, malicious actors have heightened their efforts as well. This year's version of the Guide has been refreshed and updated throughout, but there are two significant additions in the 2020 Guide that are worth special emphasis. First, Section 3 contains a new and significant "Year in Review" discussion of how the botnet threat has evolved over the past year. Some of the key takeaways of our analysis include:

- ▶ Botnets are increasingly adopting strategies that make them more effective at causing damage while avoiding detection.
- ▶ Botnets are more frequently targeting enterprise IoT and other IoT devices with more complex processors and architectures.
- ▶ Cryptocurrency botnets are on the rise, and the operators of these botnets often compete fiercely with one another.
- ▶ Botnets are increasingly used for commercial and retail fraud.
- ▶ Social media bots are falsifying social proof and spreading copyrighted or illegal-to-distribute content.
- ▶ We are beginning to see IPv6 DDoS attacks, with at least one proven example.

Second, the parts of Section 5 that address Devices and Device Systems, as well as Home and Small Business Systems Installation, have benefited from the CSDE's development of the world's leading industry consensus on IoT security. Leveraging technical input from hundreds of security experts across thousands of different companies, the CSDE convened 20 major cybersecurity and technology organizations, industry associations, consortia, and standards bodies to identify baseline security requirements for the rapidly growing IoT marketplace. This effort, known as "Convene the Conveners" or "C2", sought to address four challenges:

1. Promoting global harmonization to prevent fragmentation of security specifications and requirements.
2. Working with emerging global market forces that naturally favor secure devices and systems.
3. Developing a coherent common language on these issues that is compelling to various policy and technical audiences.
4. Assisting policy development internationally and in the United States, including at the state level.

The result of this landmark effort, the *C2 Consensus on IoT Device Security Baseline Capabilities*, or "C2 Consensus Baseline," was released on September 17, 2019. The C2 Consensus Baseline is a common set of device security capabilities that can be applied to all new IoT devices that connect to the internet — best-practice capabilities that are broadly applicable, vertically and horizontally, across markets. It applies to the diverse range of new IoT devices, accommodating the broad spectrum of device complexity, regardless of the deployment environment. The baseline is intended to be flexible and not prescriptive. Depending on a variety of factors — including device

complexity, device manageability, risk profile, use case, and context — the security capabilities outlined in the baseline can be achieved in a variety of ways, with the key being that the ultimate baseline capability is achieved in a manner applicable to the specific device.

Also informing the Guide this year is NIST's extensive multistakeholder process on baseline IoT device security. The draft NISTIR 8259<sup>1</sup> and the C2 effort are in material agreement on baseline device capabilities, with additional recommendations for organization capabilities, customer information and lifecycle activities on both sides.

Finally, we must highlight that the CSDE's member companies also developed a blueprint for industry coordination in the event of a massive botnet attack, informed by the 2016 Mirai IoT-based botnet incident that took down significant portions of the internet in the US and Europe. This blueprint is included in our report *Cyber Crisis: Foundations of Multi-Stakeholder Coordination* or "Cyber Crisis Foundations". The report considers strategies for a total of 12 significant cybersecurity events.

**Activating Shared Responsibility to Secure the Global Digital Economy.** The digital economy has been an engine for commercial growth and quality-of-life improvements across the world.

But no single stakeholder — in either the public or private sector — controls this system. Rather, securely managing the opportunities presented by this growth is the challenge and responsibility of every stakeholder in the Information and Communications Technology (ICT) community.

In recent years, however, botnets have become particularly and increasingly damaging and costly to the digital economy. Botnets are large networks of compromised, internet-connected computers and devices that malicious actors can command to commit distributed denial of service (DDoS) attacks, propagation of ransomware, phishing attacks, and disinformation campaigns amplifying inauthentic social media, and other malicious acts.<sup>2</sup> Unfortunately, as the number of connected people, businesses, and devices grows, so does the potential for these malicious attacks. Today, the destructive potential of botnets has increased exponentially as they attack and leverage the billions of Internet of Things (IoT) devices, estimated to reach 20 billion connected devices by 2020. With this substantial and growing attack surface, it is no coincidence that the global cost of cyber-crimes is expected to reach trillions of dollars. Botnets are the industrial-scale driver of these losses, and they are a persistent threat that will seek to evolve and adapt in the years to come.

**IBM Security Intelligence reports that activity from Mirai variants almost doubled between 2018 and 2019.**

This Guide aims to reverse these trends. While the developers of this Guide strongly support the important role that governments play in convening a diverse ecosystem, the imposition of prescriptive, compliance-focused regulatory requirements will inhibit the security innovation that is key to staying ahead of today's sophisticated threats. Moreover, earlier policy efforts were based on utopian solutions to these threats, premised on the notions that internet service providers (ISPs) can simply shut down all botnets, or that manufacturers can make all devices universally secure. Instead, dynamic, flexible solutions that are informed by voluntary consensus standards, driven by market demands, and implemented by stakeholders throughout the global digital economy, are the better answer to these evolving systemic challenges.

To enable such solutions and encourage the sharing of responsibility among all stakeholders, this Guide sets forth a set of *baseline practices* that various stakeholders should implement; further, it highlights additional *advanced capabilities* that are presently available but underutilized. Widespread implementation of the security practices featured in this Guide will dramatically reduce botnets and help secure the global digital economy. The Guide provides real-world, presently available solutions to a global challenge that cannot be met by one stakeholder set or one country alone or by any governmental mandate. The Guide is informed by an ongoing collaboration with companies across multiple industries and countries to dramatically reduce the botnet threat, and by an analysis of rapidly evolving global threats and vulnerabilities, as well as increasingly capable and determined adversaries.

The Guide is premised on, and affirmatively seeks to advance, the following core security principles:

- ▶ Security demands dynamic, flexible solutions that are driven by powerful global market forces and are as nimble and adaptable as the cyber threats that need to be mitigated, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.
- ▶ Security is a shared responsibility among all stakeholders in the internet and communications ecosystem.
- ▶ Government and industry stakeholders should promote solutions that increase responsibilities among all players, rather than seeking facile solutions among certain select components or stakeholders.
- ▶ Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, through collective action against bad actors and rewards for the contributions of responsible actors.

These principles are the foundation of the new approach to botnet mitigation that circumstances demand.

**The International Botnet and IoT Security Guide: Summary of Practices and Capabilities.** The complexity and diversity of the “system of systems” comprising the internet and associated communications ecosystem makes it impossible to provide a set of guidance that uniformly applies to all stakeholders. The Guide groups these diverse components based on five constituent types of provider, supplier, and user stakeholders: (1) Infrastructure, (2) Software Development, (3) IoT Devices, (4) Home and Small Business Systems Installation, and (5) Enterprises. For each of these components, the Guide lays out baseline practices that all such stakeholders should aspire to meet, as well as advanced capabilities that are presently available — if underutilized — in the marketplace. These practices and capabilities, summarized briefly below, are the core of this Guide.

1. **Infrastructure.** For purposes of this Guide, “infrastructure” refers to all systems that enable connectivity and operability — not only to the physical facilities of providers of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and other services, but also to the software-defined networks and other systems that reflect the internet’s evolution from tangible things to a digital concept. We recommend baseline practices and advanced capabilities for infrastructure to include:
  - Detect Malicious Traffic and Vulnerabilities
  - Mitigate Against Distributed Threats
  - Coordinate with Customers and Peers
  - Address Domain Seizure and Takedown



2. **Software Development.**<sup>3</sup> Software is an increasingly ubiquitous element of every other component of the ecosystem. There are a wide variety of complex development processes and interdependencies that drive software innovation and improvement. We recommend that software generally consist of baseline practices and advanced capabilities to include:
  - Secure-by-Design Development Practices
  - Security Vulnerability Management
  - Transparency of Secure Development Processes
3. **IoT Devices.** An individual connected device (or “endpoint device”) may itself consist of multiple components, including hardware modules, chips, software, sensors or other operating components. Beyond the individual device itself are multiple additional layers of connectivity that constitute a highly dynamic new market — including for security innovation. For the endpoint “things” in the IoT, we recommend baseline practices and advanced capabilities to include:
  - Secure Development
  - Secure Capabilities
  - Product Lifecycle Management
4. **Home and Small Business Systems Installation.**<sup>4</sup> Homes and small businesses benefit from connected devices in several categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others. Drawing heavily from The Connected Home Security System,<sup>5</sup> we recommend baseline practices and advanced capabilities to include:
  - Authentication and Credential Management
  - Network Configuration
  - Network Hardware Management
  - Security Maintenance
5. **Enterprises.**<sup>6</sup> As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, non-profit — have a critical role to play in securing the digital ecosystem. For enterprises, we recommend baseline practices and advanced capabilities to include:
  - Secure Updates
  - Real-time Information Sharing
  - Network Architectures that Securely Manage Traffic Flows
  - Enhanced DDoS Resilience
  - Identity and Access Management
  - Mitigating Issues with Out-of-Date and Pirated Products

**Looking Ahead.** Just as the publication of the 2018 Guide was only a first step, this Guide is part of the CSDE's ongoing strategy to engage a broad set of stakeholders, including governments of like-minded countries, to promote baseline practices and advanced capabilities, and we will continue looking ahead to what the evolving threat requires. As stated in the 2018 Guide, we will update, publish and promote a new version of the Guide annually. Starting this year, the title of our Guide reflects the upcoming year, hence this is the 2020 edition.

While the hallmark of this year's efforts to combat botnets is IoT device security, based on the urgent need for a widely accepted baseline, not all significant botnets target connected devices — in fact, some of the world's most destructive botnets do not target connected devices at all. So, while it is clear that the future of botnets is closely intertwined with the future of IoT security, and the CSDE will continue to lead on this front, we will also explore other ways that botnets and other distributed threats can be reduced dramatically through our members' leadership. In recognizing the complex and layered nature of the botnet threat, the companies in the CSDE will engage these threats on multiple fronts.

**The digital economy has been an engine for commercial growth and quality-of-life improvements across the world and may already represent 20% of global economic value.**

## 02 / Introduction

The members of the Council to Secure the Digital Economy (CSDE) cover the entirety of the complex global internet and communications ecosystem. These organizations count among their members companies that provide the human and technical systems that create, manage, and install connectivity capabilities, software, and devices that benefit a significant portion of the world's consumers, small businesses, large private enterprises, governments, and non-profits — collectively, the global digital economy.

Since producing the *International Anti-Botnet Guide 2018*, CSDE members — Akamai, AT&T, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefónica, and Verizon — supported by USTelecom and the Consumer Technology Association (CTA), have been driving the adoption of improved security in the global marketplace across infrastructure, software, devices, and other segments of the digital economy, in order to unite industry globally in the battle against malicious botnets.

The world has taken notice. In 2019, the UN Internet Governance Forum recognized the CSDE for taking meaningful action to combat botnets and other automated, distributed threats through a collaborative, whole-of-ecosystem approach, where security is a shared priority. We were also recognized in the US Government's Botnet Roadmap as key contributors to the fight. Our global project is having an impact in many parts of the world, including Europe, Asia, and Latin America, where CSDE members do business.

**Overview of the Challenge.** The digital economy has been an engine for commercial growth and quality-of-life improvements across the world, creating jobs and opportunities on every continent. By some estimates, it may already represent 20% of global economic value.<sup>7</sup> While GDP alone cannot capture the full contributions of the digital economy to global economic value — not all value provided digitally involves a commercial transaction — *The Wall Street Journal* reports that the digital economy was worth \$11.5 trillion in 2016 and may increase to \$23 trillion, nearly a quarter of global GDP, by 2025.<sup>8</sup> The digital economy's growth is continuously fueled by business and consumer adoption of new and emerging technologies.<sup>9</sup> Securely managing the opportunities presented by this impressive growth is the challenge and responsibility of every stakeholder in the Information and Communications Technology (ICT) community.

In recent years, however, botnets have become particularly and increasingly damaging and costly to the digital economy. They are able to propagate malware,<sup>10</sup> conduct denial of service attacks,<sup>11</sup> and spread corrosive disinformation artificially on social media.<sup>12</sup> A single botnet can now include more than 30 million “zombie” endpoints and allow malicious actors to profit six figures per month.<sup>13</sup> More systems are vulnerable today than ever before, due to the tremendous and otherwise promising growth of the digital economy itself — particularly regarding the rapid deployment of billions of Internet of Things (IoT) devices, estimated to reach 20 billion connected devices by 2020.<sup>14</sup> The benefits of this connected economy are revolutionizing businesses and consumer activities for the good, and the companies that have developed this Guide are innovating new security measures as they deploy devices. Nevertheless, insecure devices continue to stream into the marketplace without systems in place that are designed to secure them.<sup>15</sup> Moreover, it is now possible for relatively unskilled malicious actors to rent a powerful botnet for large-scale nefarious activities.<sup>16</sup>

These developments inflict direct, tangible costs on the digital economy. For example, since 2017, malware has spread across Europe, Asia, and the Americas, causing more than \$10 billion in damage.<sup>17</sup> It is estimated that over the next five years cyber-crimes alone will globally cost businesses a cumulative total of \$8 trillion (in fines, loss of business, remediation costs, etc.).<sup>18</sup>

The intangible costs are just as detrimental, as these threats undermine fundamental confidence and trust in the digital economy.

**Strategic Posture and Goals.** We aim to reverse these trends. While we recognize and support the important convening role that governments can play in helping to channel the activities of the diverse players in the ecosystem, we also believe that compliance-based regulatory requirements actually inhibit the security innovation that is required to stay ahead of today's sophisticated threats. In other words, not only are prescriptive regulatory requirements rarely effective, but they are in fact usually counterproductive to the goal of security.<sup>19</sup> Dynamic, flexible solutions that are informed by voluntary consensus standards, driven by market demands, and implemented by stakeholders throughout the global digital economy are the better answer to evolving systemic challenges like malicious botnets that threaten all players in this complex ecosystem.

Therefore, this Guide seeks to empower responsible participants in the digital economy to secure its future and leverage its full potential. We believe that active collaboration and collective action will be commercially beneficial for all stakeholders, large and small, over the long term. To that end, this Guide may be used to increase the resilience of the internet and communications ecosystem and enhance the transactional integrity of the underlying digital infrastructure. The Guide urges all stakeholders in this global digital marketplace to implement a set of baseline tools, practices, and processes; further, it highlights additional advanced capabilities that are presently available — but perhaps still underutilized. Widespread implementation of the security practices featured in this Guide will dramatically reduce botnets and help secure the global digital economy.

Publication of the 2018 Guide was only a first step. We are presently engaging a broad set of stakeholders, including governments of like-minded countries, to promote the Guide's baseline practices and advanced capabilities. Further, we will continue to update, publish, and promote a new version of the Guide annually.

**New Material in the 2020 Guide.** This year's version of the Guide has been refreshed and updated throughout, but there are two significant additions in the 2020 Guide that are worth special emphasis. First, Section 3 contains a new and significant "Year in Review" discussion of how the botnet threat has evolved over the past year. Some of the key takeaways of our analysis include:

- ▶ Botnets are increasingly adopting strategies that make them more effective at causing damage while avoiding detection.
- ▶ Botnets are more frequently targeting enterprise IoT and other IoT devices with more complex processors and architectures.
- ▶ Cryptocurrency botnets are on the rise, and the operators of these botnets often compete fiercely with one another.
- ▶ Botnets are increasingly used for commercial and retail fraud.

- ▶ Social media bots are falsifying social proof and spreading copyrighted or illegal-to-distribute content.
- ▶ We are beginning to see IPv6 DDoS attacks, with at least one proven example.

Second, the parts of Section 5 that address Devices and Device Systems, as well as Home and Small Business Systems Installation, have benefited from the CSDE's development of the world's leading industry consensus on IoT security. Leveraging technical input from hundreds of security experts across thousands of different companies, the CSDE convened 20 major cybersecurity and technology organizations, industry associations, consortia and standards bodies to identify baseline security requirements for the rapidly growing IoT marketplace. This effort, known as "Convene the Conveners" or "C2", sought to address four challenges:

1. Promoting global harmonization to prevent fragmentation of security specifications and requirements.
2. Working with emerging global market forces that naturally favor secure devices and systems.
3. Developing a coherent common language on these issues that is compelling to various policy and technical audiences.
4. Assisting policy development internationally and in the United States, including at the state level.

The result of this landmark effort, the *C2 Consensus on IoT Device Security Baseline Capabilities* or "C2 Consensus Baseline," was released on September 17, 2019. The C2 Consensus Baseline is a common set of device security capabilities that can be applied to all new IoT devices that connect to the internet — best-practice capabilities that are broadly applicable, vertically and horizontally, across markets. It applies to the diverse range of new IoT devices, accommodating the broad spectrum of device complexity, regardless of the deployment environment. The baseline is intended to be flexible and not prescriptive. Depending on a variety of factors — from device complexity, device manageability, risk profile, use case and context — the security capabilities outlined in the baseline can be achieved in a variety of ways, with the key being that the ultimate baseline capability is achieved in a manner applicable to the specific device.

**Based on a study of 180 countries and territories, Verizon reported that 84% of botnets involved in data breaches targeted the finance and insurance industries.**

Also informing the Guide this year is NIST's extensive multistakeholder process on baseline IoT device security. The draft NISTIR 8259<sup>20</sup> and the C2 effort are in material agreement on baseline device capabilities, with additional recommendations for organization capabilities, customer information and lifecycle activities on both sides.

Finally, we must highlight that the CSDE's member companies also developed a blueprint for industry coordination in the event of a massive botnet attack, informed by the 2016 Mirai IoT-based botnet incident that took down significant portions of the internet in the US and Europe. This blueprint is included in our report *Cyber Crisis: Foundations of Multi-Stakeholder Coordination* or "Cyber Crisis Foundations". The report considers strategies for a total of 12 significant cybersecurity events.



## 03 / The Evolution of Botnets: Year in Review

As was the case upon publication of the *International Anti-Botnet Guide 2018*, the most prominent category of automated, distributed threats to the global internet and communications ecosystem is botnets — large networks of compromised internet-connected computers and devices that communicate with servers that have command-and-control capabilities.

Botnets spread themselves globally through malware that scans the internet for insecure networks, computers, and other connected devices. When a botnet has compromised a sufficient number of devices, criminals and other bad actors can command them to commit a broad variety of nefarious acts such as distributed denial of service (DDoS) attacks, propagation of ransomware, phishing attacks, and disinformation operations that artificially amplify inauthentic social media posts.<sup>21</sup>

**Botnets: A Persistent Global Problem.** As the companies in the CSDE work continuously with the global community to put ever-increasing pressure on botnet operators, these malicious actors are not idle. They do not want to see their operations dismantled, and they see our companies' actions are a direct threat to profits and other critical objectives. Over the course of 2019, we have observed a variety of trends that lead us to conclude that, while progress is being made in the fight against botnets, the challenges are escalating.

Our adversaries are paying attention to every move we make and intelligently evolving their strategies in response. Botnet operators constantly invent new tools, adopt new techniques, and study how we combat their disruptive bots, in order to fight back against our efforts. We are grappling with highly motivated and increasingly sophisticated enemies, including nation states and large-scale criminal organizations, which are very well-financed. These organizations have effectively shielded themselves from attribution, while standing to make enormous ill-gotten financial gains through criminal methods.

In this section, we will review how the botnet threat has evolved over the past year. Some of the key takeaways of our analysis include:

- ▶ Botnets are increasingly adopting strategies that make them more effective at causing damage while avoiding detection.
- ▶ Botnets are more frequently targeting enterprise IoT and other IoT devices with more complex processors and architectures.
- ▶ Cryptocurrency botnets are on the rise, and the operators of these botnets often compete fiercely with one another.
- ▶ Botnets are increasingly used for commercial and retail fraud.
- ▶ Social media bots are falsifying social proof and spreading copyrighted or illegal-to-distribute content.
- ▶ We are beginning to see IPv6 DDoS attacks, with at least one proven example.

**Mirai Won't Die: Over 60 Variants, Activity Nearly Doubles.** Since the Mirai botnet's source code was leaked online three years ago, malicious actors have continuously experimented and created their own upgraded versions. As of July 2019, the Mirai botnet has at least 63 confirmed variants<sup>22</sup> and it is very possible others remain undiscovered.

IBM Security Intelligence reports that activity from Mirai variants *almost doubled* between 2018 and 2019.<sup>23</sup> In an interview about new IoT exploits, published in March 2019, a researcher at AT&T Cybersecurity stated, "Whenever we look at new IoT malware — it's almost inevitably a new Mirai variant. Every day we see new Mirai variants with different payloads..."<sup>24</sup> Mirai-related activity had decreased after a historic cyberattack in 2016 that shut down significant portions of the internet in the US and Europe, but this resurgence indicates the malware continues to be a serious threat.

The different Mirai variants are controlled by operators who compete among themselves for dominance of vulnerable IoT devices. As can be expected given the technological arms race that botnet operators fight on multiple fronts — against law enforcement and against each other — the newer botnets are generally more resourceful than Mirai.<sup>25</sup> Echobot, for instance, is a Mirai variant discovered in 2019 that uses at least twenty-six exploits to infect devices.<sup>26</sup>

In some instances, botnet creators will combine the Mirai code with code from other sources to achieve their ends. For example, Gafgyt, which according to IBM X-Force data accounts for 27% of all malware targeting IoT devices,<sup>27</sup> is generally regarded and studied as separate from Mirai, despite sharing part of its leaked source code.

*The CenturyLink 2019 Threat Report*<sup>28</sup> contains a side-by-side of Gafgyt, Mirai, and other IoT botnet malware based on data from CenturyLink's Black Lotus Labs.<sup>29</sup> The data reveals that average uptime for both Gafgyt and Mirai are decreasing. Explanations include that more researchers and threat teams are tracking the malware's movement; threat researchers are getting better at identifying IoT malware variants that are designed to evade detection; and providers are getting better about proactively tracking threats on their networks.<sup>30</sup>

**Enterprises and High-Complexity Devices at Increased Risk.** While enterprises have always been an important part of the whole-of-ecosystem approach to reducing botnets, they increasingly stand to incur damages and losses. We are seeing a rapid expansion of the botnet threat landscape, and recent IBM X-Force data reveals that enterprise systems are being infected with greater frequency by Mirai variants.<sup>31</sup> Data from Telefónica suggests that businesses are most likely to be infected by a botnet during the initial two months after a new service is deployed.<sup>32</sup>

Data breaches are facilitated by botnets so often that Verizon's *2019 Data Breach Investigation Report* analyzed botnet attacks separately "to avoid eclipsing" other types of incidents. Any industry can be targeted. However, some industries are clearly at higher risk to botnet attacks. Based on a study of 180 countries and territories, Verizon reported that 84% of botnets involved in data breaches targeted the finance and insurance industries; 10% targeted information industries;<sup>33</sup> and 5% targeted professional, scientific, and technical services industries. The study did not differentiate between IoT botnets and other botnets.

In the past, IoT-based botnets mostly infected connected devices and systems found in the home, such as cameras, video recorders, lighting fixtures, and thermostats. But it only makes sense that, from the criminal's perspective, any new category of IoT device — whether in the home, at the enterprise level, or elsewhere in the ecosystem — is a new battalion in their botnet army. Many stakeholders with connected devices, not just enterprises, are at increased risk.

For example, over the course of 2019, CenturyLink's Black Lotus Labs has been profiling TheMoon, an IoT botnet that targets router vulnerabilities in broadband networks.<sup>34</sup> Although this particular threat has been mitigated, it shows how IoT security has implications for infrastructure and the ecosystem as a whole.

In February 2019, security researchers discovered Mirai samples affecting a collection of processors and architectures that previously could not be targeted.<sup>35</sup> We can now expect infections of more types of routers, networked sensors, radios, and microprocessors for digital signals.<sup>36</sup> Developments like these open the door to larger botnets.

Experts believe that future attack vectors may increasingly include industrial IoT systems and connected wearables,<sup>37</sup> so it will be essential for industry and government to coordinate on identifying security capabilities that recognize the unique considerations associated with different levels of complexity.

**Intelligent, Automated Botnets: Swarmbots and Hivenets.** Picture thousands of bees swarming a single target. That, in essence, is a swarmbot. Swarmbots can often overwhelm traditional defenses through sheer volume alone.<sup>38</sup> To make matters worse, these bots are directed by an artificial intelligence known as a hivenet.

Hivenets are “botnets that think for themselves” and have the ability to learn during an attack.<sup>39</sup> The ability to learn in real-time is a big part of what makes them dangerous. Whereas traditional botnets needed to wait for commands from their operators,<sup>40</sup> the hivenet coordinates strategies automatically based on what the swarmbots learn.

Swarmbots share information about vulnerabilities discovered and other strategic information to increase the hive's collective intelligence. The bots also coordinate and share resources automatically. Individual bots may be equipped with different tools; when the hivenet discovers a vulnerability, the swarmbot with the right tool for the job is mobilized.<sup>41</sup>

By deploying swarm-based technology, botnet operators can significantly increase the efficiency of an attack by reducing the time needed to infiltrate a device or device system. One of the main reasons criminals need greater efficiency is to outperform network security tools that are being deployed with increasing frequency throughout the global marketplace.<sup>42</sup> We are in a long-term technological arms race, and swarm-based technology is the criminals' effort to escalate because their old tools increasingly prove ineffective.

**Emotet Is Back with More than 200,000 Stolen Emails and Passwords.** Cisco's Talos reports that after a hiatus of several months, the botnet Emotet returned with a vengeance in September 2019.<sup>43</sup> Emotet spews spam at a high volume to users across the world, tricking them into unleashing malicious payloads, now including the TrickBot Trojan and Ryuk Ransomware, which are both known for burrowing deep into victims' networks, increasing damage potential.<sup>44</sup>

NTT is currently using netflow data captures, and leveraging insight into 40% of global internet traffic, to analyze the infrastructure and threat actors behind TrickBot, which by the end of last year became recognized as the top threat to businesses.<sup>45</sup> Since TrickBot is often downloaded after infection with Emotet, mitigating TrickBot can help limit Emotet's destructive potential.

Often, emails sent by Emotet appear to come from legitimate contacts. The emails may include details from real conversations recipients participated in. Emotet is known to quote previous email threads and even send follow-up emails like a human being would. Tactics like these make the botnet increasingly difficult for spam filters and human beings to detect.<sup>46</sup>

Emotet gets the information necessary to deceive email recipients by breaking into email accounts and stealing the contact lists and emails from victims' computers. In its study of Emotet, Cisco's Talos discovered 202,675 unique username-password combinations.<sup>47</sup> Cisco's Talos also reports that when analyzing Emotet inside a malware sandbox known as Threat Grid for 10 months, the malicious botnet attempted to send spam nearly 19,000 times.<sup>48</sup>

While tech news publications have referred to Emotet as "the world's most destructive botnet"<sup>49</sup> and "today's most dangerous botnet",<sup>50</sup> it is not the only high-volume spambot currently active. For instance, Gamut and Necurs, spambots that just a few years ago accounted for 97% of spam traffic on the internet, continue to cause trouble.<sup>51</sup>

As of 2019, Cisco reports the Gamut botnet has been sending out dating and intimate relations spam, as well as ads for pharmaceuticals and job opportunities.<sup>52</sup> Necurs has evolved from a botnet that delivers banking trojans and ransomware to also enabling proxying traffic, cryptomining, and launching DDoS attacks. Analysis by CenturyLink reveals Necurs is seen primarily in developing nations.<sup>53</sup> However, because botnets ignore jurisdictional boundaries, these infections can have significant spillover effects in all parts of the world.

**Botnets for Rent: Now Available on Both the Dark Web and Social Media.** Throughout the dark web — areas of the internet accessed using specific software — criminal marketplaces exist where botnets can be rented for a low fee by cybercriminals. This arrangement, called malware-as-a-service (MaaS), puts destructive tools into the hands of a broader set of malicious actors.<sup>54</sup> Some of the criminals who rent a botnet lack the technical skills to make a botnet of their own. However, others see renting a botnet as purely a pragmatic business decision. Like legitimate businesses, criminal enterprises are interested in return on investment and are willing to prioritize investments that yield the highest returns.<sup>55</sup> Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.

In the 2019 Cyber Crisis Foundations report, the CSDE documents the case of a Liberian telecom company that became the subject of a lawsuit after hiring a criminal hacker to launch DDoS attacks against a rival to gain an unfair competitive advantage.<sup>56</sup> The hacker used a custom botnet based on Mirai and rented infected security cameras and routers from other hackers.<sup>57</sup> At their peak, the attacks *disabled access for most internet users in the country*, further adding to global concerns about IoT security.<sup>58</sup>

Lest you think all malicious activity unfolds in the secrecy of the dark web, increasingly botnet creators are advertising their creations on mainstream platforms. Sometimes, creators will even rent out botnets that are

still in development, as eager criminals line up to secure a spot. For example, the creators of Cayosin — a botnet described as “Frankenstein” because it is made from different pieces of open source malware (including Mirai) — have advertised their project on YouTube and Instagram, openly flouting the law and charging a low rental fee to incentivize criminals to become their customers.<sup>59</sup>

By using social media, botnet creators are able to conduct market research with the goal of increasing their profit — they sometimes openly ask for customer feedback on the services provided, so they can improve service and build a relationship with their criminal customers.<sup>60</sup> This is a marked shift in the cultural evolution of botnet criminals.

**Stealthy Bots Use Tricks to Avoid Detection.** Botnet developers are constantly evolving their strategies to keep bots hidden and active longer. A recent Akamai report explains, “Bots can represent up to 60% of overall web traffic, but less than half of them are actually declared as bots — making tracking and blocking difficult.”<sup>61</sup> A further complicating factor is that not all these bots are malicious, making it challenging to root out criminal behaviors when automation is detected.

For example, to avoid detection when visiting a website, malicious bots impersonate popular browsers and mobile applications, or in some cases they pretend to be good bots.<sup>62</sup> Some bots tamper with browser properties to spoof “fingerprint characteristics” which tend to be whitelisted or tamper with cookies, either by dropping the cookies or even harvesting good cookies to appear legitimate.<sup>63</sup>

We have also seen the continued rise of “low and slow attacks”, where bots try to stay under the radar, unwearingly stealing a large amount of information over time.<sup>64</sup> When using this method, bots will change their IP addresses or use multiple IP addresses. This allows the bots to bypass rate limitations without being noticed; multiple IP addresses send a small number of requests per hour.<sup>65</sup>

Bots are also using other techniques to get around rate limits when staying “low and slow”. With greater frequency, botnet operators anonymize malicious traffic by routing it through residential broadband and wireless connections.<sup>66</sup> Botnets have also been morphing their IP addresses via proxies by hiding in anonymous networks, such as VPNs and Tor<sup>67</sup> — including a recently discovered Mirai variant.<sup>68</sup> When your enemy can hide in the crowd, without exposing itself, the job of detecting and defending against the enemy is considerably more difficult.

Botnets have been making use of another trick — essentially, playing dead. The Necurs botnet analyzed by CenturyLink’s Black Lotus Labs goes into sustained downtime at various intervals. In one observed instance, Necurs was active for three weeks, went quiet for two weeks, and then activated again.<sup>69</sup> In 2019, Necurs appeared largely inactive for several months, only springing into action about once per week for brief periods of time.<sup>70</sup> Necurs proved resistant to various sinkholing attempts — traps for botnets deployed by law enforcement or security researchers — due to its domain generational algorithm (DGA). However, analyzing the botnet’s DGA reveals to researchers which domains will be generated in the future, so they are able to inspect relevant DNS and network traffic and deploy mitigation strategies.<sup>71</sup>

**Bots Defraud Online Retailers and Advertisers, Pretend to Be Human.** A recent Akamai *State of the Internet Security* report<sup>72</sup> reveals that malicious bots now account for nearly half of the internet bandwidth directed at online retailers.<sup>73</sup> In light of this sobering fact, the report refers to bots as “tools of mass (retail) destruction”.



For years, criminals have used botnets to perpetrate ad fraud by sending bots instead of real human eyes to online destinations. This costs advertisers millions of dollars and provides users with worse web browsing experiences.<sup>74</sup> Bots have also been used in other profit-driven activity, such as buying popular merchandise or tickets to popular events and scalping them.<sup>75</sup>

Earlier this year, Oracle's security experts uncovered a major fraud operation involving DrainerBot, which spread via a software development kit (SDK) found in hundreds of mobile phone apps and games. The infected apps, once installed on unsuspecting users' phones, would use more than 10 GB of data every month (even if the phone was in sleep mode) and trick advertisers into thinking they were getting human traffic.<sup>76</sup>

In 2019, it is much more difficult to tell whether online activity is human. In the past, if suspicions were raised, it was relatively easy to identify non-human behaviors such as opening and closing millions of windows.<sup>77</sup> However, malicious bot activity increasingly resembles real human web browsing, such that even experts have trouble telling the difference.

**Social Botnets Spread Disinformation and Illegal Links.** The ability of botnet traffic to resemble ordinary human traffic has implications beyond defrauding retailers and advertisers. Botnets are abusing social media in a number of different ways, from impersonating millions of people to facilitating access to copyrighted or illegal-to-distribute content.

In last year's guide, we observed that botnets can play a role in the spread of corrosive disinformation that may deprive the public of an opportunity to make informed decisions. Bots that imitate human behavior could potentially be used to influence human opinions on just about any topic, from musical trends to politics, by falsifying social proof.<sup>78</sup>

For a common example of botnets spreading copyrighted content, we can look to sports. In December 2018, Telefónica published a trend report on "Twitter botnets detection in sports events".<sup>79</sup> The bots massively disseminate links to illegally streaming content, interfering with the profits of the rights holders.

Curtailling botnets that exploit social media will be no easy task. In September 2019, Twitter's transparency report revealed that the platform had removed thousands of accounts with apparent connections to state-backed social media campaigns.<sup>80</sup> Altogether, the platform has purged millions of fake accounts.<sup>81</sup> Yet botnets are constantly learning, adapting, and being upgraded to evade bans and continue their operations undetected.

**Bots Surge to Mine for Anonymous Cryptocurrency.** The rise of cryptocurrency has become fuel for botnet activity. In 2018, the Cyber Threat Alliance found a 459% increase in cryptomining malware,<sup>82</sup> and it is possible that by the end of 2019 we will be faced with similarly shocking figures.

Botnet mining operations are driven by profit. So, when the cryptocurrency Monero tripled in value in Summer 2019, there was a noticeable surge in botnet activity.<sup>83</sup> In general, criminals prefer cryptocurrencies such as Monero and ZCash that are relatively anonymous, rather than bitcoin which is easier for law enforcement to trace.<sup>84</sup>

Although victims' infected systems will generally continue to function, the crime is not victimless; the added stress on IT infrastructure can have severe consequences, including physical damage.<sup>85</sup> Victims may notice slower performance and increased lag time because resources are being diverted to the task of profiting criminals. Business operations may be negatively impacted and victims may notice higher energy bills.<sup>86</sup>

**Botnet Turf Wars Move to the Cloud.** The competition among criminals to take over as many devices and systems as possible quite frequently leads to botnet “turf wars”. Botnets infect devices already infected by other botnets — and delete their rivals — in order to increase their own power and profits.

In 2019, we saw an escalation of the rivalry between Rocke and Pascha, cryptomining hacking groups that compete for dominance over the Linux cloud computing environment.<sup>87</sup> Both groups use ill-gotten cloud resources to advance cryptomining operations. Meanwhile, Smominru, another cryptomining botnet, has been deleting rivals from Windows 7 computers.<sup>88</sup> Whereas two more cryptomining bots, Fbot and Trinity, continued a fight that began last year to control tens of thousands of unsecured Android devices.<sup>89</sup>

As bots that delete other bots become more common, and profits are at stake, there is significant pressure on botnet operators to fight their rivals using the latest tools, or at least take steps to defend themselves. For example, some botnets will actively patch security vulnerabilities after they break into a device, in order to prevent a rival from breaking in.

The demand for powerful botnets that can shut down their rivals has been reflected in criminal marketplaces on the dark web, resulting in the proliferation of powerful malware like Mylobot, which has an unprecedented number of tools at its disposal.<sup>90</sup>

As criminal hackers worry about rivals making them obsolete, they also need to consider the threat posed to their operations by “cyber vigilantes”. Botnets like BrickerBot<sup>91</sup> and Hajime<sup>92</sup> were designed to erase malicious botnets and ostensibly improve the security of an infected system. Although the intentions behind these botnets are not on the surface malicious, the vigilante botnets are nonetheless breaking the laws of many countries.

**Sometimes, criminals with advanced technical proficiency will rent botnets to supplement their already-existing armies — in these cases, one can think of the rented botnets as mercenaries.**

**Future of IPv6 Security and the Internet of Things.** IPv6 is an internet protocol defined by the Internet Engineering Task Force (IETF)<sup>93</sup> and was created to replace the older IPv4 protocol over time.<sup>94</sup> As the number of internet users and connected devices grows across the globe, networks are increasingly providing IPv6 connectivity,<sup>95</sup> and in many cases IPv6 and IPv4 are deployed together.

Akamai's *State of the Internet Security* notes, however, that “[b]ecause IPv6 is still seen as a minority of traffic, it’s not a major selling point for a number of security tools. Not all organizations consider the IPv6 space worth monitoring, even when the capability is present.”<sup>96</sup>

Botnets like Mirai gain new bots through automated scans of the IPv4 address space, and vulnerable devices are usually infected within a few minutes of connecting to the internet.<sup>97</sup> By contrast, scanning the IPv6 address space has been considered extremely difficult due to the sheer size.<sup>98</sup> Nonetheless, for years, experts have been warning that undiscovered vulnerabilities in the IPv6 protocol, combined with the growth of IoT, could allow for massive botnet attacks.<sup>99</sup>

There is now at least one documented case of an IPv6 DDoS attack, which used a technique known as DNS amplification instead of a botnet.<sup>100</sup> While it did not amount to a major incident, the question must be asked: could IPv6 result in more and bigger DDoS attacks over time? The rise of IPv6 botnet attacks would present unique challenges that have no easy fix. For instance, the incredibly large number of IPv6 addresses (over 8,000 times more than IPv4) could allow attackers to overwhelm the memory of security systems designed to handle IPv4-based threats.<sup>101</sup>

**Conclusion.** While industry makes tangible advances in the fight against botnets, the threat has continued to evolve and grow. In the near future, global security concerns about botnets could be exacerbated by cloud migration and the growth of IoT — both developments radically increase the attack surface malicious actors can target. What we need to fight this rapidly evolving threat is a global, market-based movement toward increased security across all segments of the digital economy. At the same time, we need policies that encourage innovation and allow industry to evolve as flexibly and dynamically as the adversaries.

## 04 / Addressing Automated, Distributed Threats in a Diverse Internet Ecosystem

The fundamental challenge of addressing botnets in the highly diverse, complex, and interdependent global internet ecosystem remains: the essential nature of the internet is non-hierarchical and hyper-connected. No single stakeholder — government or private sector — controls this system, and yet we rely on it to connect all of us. Fighting malicious botnets is the classic “tragedy of the commons” challenge: If everybody has a stake in the internet commons, but nobody controls it, then who is responsible for cleaning up the malicious botnets that threaten the basic functions everyone relies on?

The answer is that all stakeholders must take responsibility — and not just for altruistic purposes of cleaning up the commons. Every entity in the ecosystem has a self-interested stake in reducing malicious botnets. Botnets are used to attack the internet on which all ICT offerings rely, and being involved in a botnet attack hurts the companies involved either by direct impact on execution or harm to reputation.

The mitigation of botnets requires a thoughtful, holistic approach. The various parts of this complex ecosystem must — for their individual and collective good — deepen and sharpen their understanding of their own responsibilities and how they complement those of others. And in cases where the lines currently are unclear or unknown, stakeholders must work together to clarify them. Absent such work, strategies for combating botnets will revert to the fallacy of utopian solutions focused on just one or two pieces of the puzzle — for instance, that ISPs should simply shut down all botnets, or that billions of devices should be made universally secure, or that consumers should become omniscient users of technology.

**A recent Akamai State of the Internet Security report reveals that malicious bots now account for nearly half of the internet bandwidth directed at online retailers.**

Such simplistic solutions have failed thus far and are unlikely to be any more successful in the future. Instead, this intricate system composed of billions of human and automated components throughout the private sector consumer and enterprise marketplaces, academia, civil society, and governments worldwide must implement mitigation methods at every level to increase its security. That is what this International Botnet and IoT Security Guide aims to do.

### What Is Different Now?

This Guide provides real-world, presently available solutions to a challenge in today’s marketplace that cannot be met by any government requirement(s) or a single country alone. We are working with global companies across multiple industries to reduce the botnet threat dramatically. We developed this Guide, informed by analysis of rapidly evolving global threats, ecosystem-wide vulnerabilities, and increasingly capable and determined adversaries, with the following consensus guiding principles in mind:

- ▶ Security demands dynamic, flexible solutions that are driven by powerful global market forces and are as nimble and adaptable as the cyber threats that need to be mitigated, rather than regulatory compliance mechanisms that differ by local or national jurisdiction.
- ▶ Security is a shared responsibility among all stakeholders in the internet and communications ecosystem. Governments and industry stakeholders should promote solutions that increase responsibilities among all players, rather than seeking facile solutions among certain select components or stakeholders.
- ▶ Security relies on mutually beneficial teamwork and partnership among governments, suppliers, providers, researchers, enterprises, and consumers, built on a framework that takes collective action against bad actors and rewards the contributions of responsible actors.

**Overview of the Global Internet and Communications Ecosystem.** As noted above, the digital economy runs on — and was made possible by — a complex global internet and communications ecosystem that is comprised of numerous systems, each of which is highly complex in its own right and highly interdependent on all of the others. And all of these different components constitute part of the ecosystem’s vulnerability to — and its resilience against — the threats posed by botnets and other automated, distributed attacks.

The complexity and diversity of the “system of systems” comprising the internet and associated communications ecosystem makes it impossible to provide a set of guidance that uniformly applies to all stakeholders. Various prominent government and private sector reports have defined and described the internet and communications ecosystem using similar yet different taxonomies that were tailored to the purposes and goals of each forum.<sup>102</sup> Rather than serving as competing visions of how the ecosystem should be understood, these definitions complement and reinforce each other.

This Guide is no exception. We group the ecosystem’s components in a manner that facilitates the identification and implementation of anti-botnet practices among its constituent groups of stakeholders. Specifically, the Guide is organized around the following five types of providers, suppliers, and users:

1. Infrastructure
2. Software Development
3. IoT Devices
4. Home and Small Business Systems Installation
5. Enterprises

To be sure, any effort to define this complex ecosystem carries some risk of being underinclusive in some way, whether actual or perceived. For instance, experience may reveal that none of the five categories listed above can reasonably accommodate some ubiquitous platforms (e.g., large social media platforms) that involve some combination of categories. For that reason, this taxonomy should be viewed flexibly with the expectation that the boundaries between systems will continue to evolve.



## 05 / Practices and Capabilities of Components of the Ecosystem

### A. INFRASTRUCTURE

For purposes of this Guide, “infrastructure” refers to all systems that enable connectivity and operability — not just to the physical facilities of providers of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and other services, but also software-defined networks and other systems that reflect the internet’s evolution from tangible things to a digital concept. We recommend baseline practices and advanced capabilities for diverse infrastructure in the modern internet and communications ecosystem.

#### Types of Infrastructure

##### ***Internet Service Providers***

An internet service provider (ISP) is an organization that provides customers a means to access the internet using technologies such as cable, DSL (digital subscriber line), dial-up, and wireless. ISPs are connected to one another through network access points, public network facilities found on the internet backbone. ISPs use these vast systems of interconnected backbone components to transfer information across long distances within seconds. ISPs may provide services beyond accessing the internet including website hosting, domain name registration, virtual hosting, software packages, and e-mail accounts. Many ISPs offer services designed to reduce botnets, including managed security solutions whereby the provider takes an active role in mitigating threats to customers. Most broadband ISPs provide antivirus as part of their offering, and many notify infected customers without any additional charges.

##### ***Internet Backbone Providers***

The internet’s backbone is a collection of vast, connected computer networks that are generally hosted by commercial, government, academic, and other network access points. These organizations typically have control over large high-speed networks and fiber optic trunk lines, which are essentially an assortment of fiber optic cables bundled together in order to increase capacity. They allow for faster data speeds and larger bandwidth over long distances, and they are immune to electromagnetic interference. Backbone providers supply ISPs with access to the internet and connect ISPs to one another, allowing ISPs to offer customers high speed internet access. The largest backbone providers are called “tier 1” providers. These providers are not limited to country or region and have vast networks that connect countries across the world. Some tier 1 backbone providers are also ISPs themselves and, due to their size, these organizations sell their services to smaller ISPs.

##### ***DNS Providers***

The Domain Name System (DNS) is essentially an address book of domain names associated with IP addresses copied and stored on millions of servers around the world. When a user wishes to visit a website and types the domain name into the search bar, the computer sends that information to a DNS server. This server (also referred to as a resolver) is usually run by the user’s ISP. The resolver then matches the domain name with an IP address

and sends the corresponding IP address back to the user's browser which then opens a connection with the webserver.

DNS providers are organizations that offer such DNS resolution services. They provide the most common DNS functions such as domain translation, domain lookup, and DNS forwarding. DNS providers also routinely update their name servers to provide the most current information.

### ***Content Delivery Networks***

A content delivery (or distribution) network (CDN) is a geographically dispersed network of data centers and proxy servers. CDN is a term used to describe many different types of content delivery services such as: software downloads, web and mobile content acceleration, and video streaming. CDN vendors may also cross over into other industries like cybersecurity with DDoS protection and web application firewalls (WAF). CDNs were designed to solve a problem known as latency, the delay that occurs between the time that a user requests a web page to the moment that its content appears onscreen. The duration of the delay typically depends on the distance between the end user and the hosting server. To shorten this duration, CDNs reduce that physical distance and improve site rendering speed and performance by storing a cached version of its contents in several locations, known as points of presence or PoPs; each PoP connects end users within its proximity to caching servers responsible for content delivery. By storing a website's content in many places at once, a company can provide superior coverage to far away end users.

### ***Cloud and Hosting Providers***

Internet hosting services enable customers to make content accessible on the internet to people and organizations throughout the world. In recent years, the increased adoption of cloud hosting services, which use remote servers hosted online instead of a local server or a personal device, has given customers access to scalable and more secure hosting solutions. Software, infrastructure, and platforms hosted on the cloud can be accessed on a subscription basis and enable customers to perform a wide variety of computing functions. Because cloud networks are decentralized, they can typically withstand the disruption of numerous network components. This architectural feature makes the cloud more resilient to highly distributed botnets and provides additional mitigation capabilities. In essence, cloud services provide an extra layer of security outside of the infrastructure provided by an ISP. This layer of protection becomes increasingly useful as the scale of botnet attacks increases. Because the cloud is upstream relative to ISPs from the target of an attack, it can mitigate the problem closer to the attack source. Cloud security services complement and do not diminish the role of ISPs in botnet mitigation.

### ***Baseline Practices and Advanced Capabilities for Infrastructure***

CSDE members take critical steps to increase the resilience of their own networks, their customers' networks, and the global ecosystem against botnets. Experts in government and industry have observed that because of the complexity of the ecosystem, no single tool will always be effective to mitigate threats,<sup>103</sup> which means that industry must retain enough flexibility to adapt to emerging threats and new technologies and tools. However, certain baseline practices have already been proven to reduce the impact of botnet-driven attacks such as DDoS attacks and should be implemented throughout the ecosystem.<sup>104</sup> Below, we identify baseline practices as well as more advanced capabilities that industry leaders use to secure the ecosystem against distributed threats.

## 1. DETECT MALICIOUS TRAFFIC AND VULNERABILITIES

The first step in mitigating distributed threats such as botnets is identifying the assets that need to be defended from attacks and the potential vulnerabilities (i.e. attack surfaces) that potentially expose these assets. Moreover, companies should stay informed about the latest exploits (i.e. attack vectors) for each identified vulnerability.

Providers can leverage trusted third-party data feeds and information-sharing mechanisms, both within their industry and across sectors. Moreover, government information-sharing mechanisms in many countries enable information to be shared between the public sector and the private sector rapidly at machine speed.<sup>105</sup>

**Summary of Baseline Detection Practices:** Providers check for known types of malware in databases that are updated regularly. A responsible company may contribute to detection efforts by sharing information on new malware with security vendors and researchers in a timely manner.

**Summary of Advanced Detection Capabilities:** Companies with access to greater resources may have a dedicated staff of security researchers that can analyze heuristics and anomalous behaviors to detect malware. The researchers' findings can be shared with other stakeholders.

### a. Signature analysis

When security experts encounter malware, they search for a unique pattern or “signature” (for example, a part of the malware’s code and the exploit code). Signature-based analysis can then be used by anyone with access to an updated database of malware signatures so that the threat can be identified regardless of where it is encountered. This sort of analysis is common in antivirus software and intrusion detection systems, and can be used to detect most malicious threats on a network. Although signature analysis is commonly used, more sophisticated malicious actors can limit the usefulness of this technique by changing the specifics of malware every time it spreads. Like a real virus, malware can adapt and evolve as it moves from host to host.<sup>106</sup> A more obvious limitation of signature analysis is that it requires foreknowledge of the malware, which means that the effectiveness of signature analysis depends on timely updates and information-sharing throughout the ecosystem. Ideally, signature analysis should be combined with other types of analysis, such as heuristic or behavioral analysis discussed below, in order to overcome the inherent limitations of this technique.<sup>107</sup>

**Baseline Practices:** Providers should ensure their signature databases are up-to-date and they should contribute to information-sharing of malware.

**Advanced Capabilities:** Providers can combine signature analysis with analysis of code heuristics (described below) and network traffic behaviors (also described below) to achieve better results.

### b. Heuristic analysis

Heuristic analysis detects malware by examining code for known signs of trouble. The code does not have to exactly match known malware to be flagged as potentially malicious. Heuristic analysis looks for many different clues in determining whether code is suspicious. In static heuristic analysis, potentially malicious code is compared to the code of malware in a database and if there are sufficient similarities then the code is flagged.

Although the possibility of false positives exists, heuristic analysis is far more effective than signature analysis at combating unknown and evolving threats. Sometimes, in order to deconstruct code safely, scientists store suspicious code that they believe to be malware inside a virtual machine called a “sandbox,” thereby preventing it from spreading to other hosts. This is known as dynamic heuristic analysis.<sup>108</sup>

**Advanced Capabilities:** Providers can detect previously unknown threats by using a combination of both static and dynamic heuristic analysis. Providers with teams of researchers can analyze suspicious code inside a sandbox to determine effective mitigation strategies, which can be shared with other stakeholders in the ecosystem.

### *c. Behavioral analysis*

Whereas signature analysis and heuristic analysis both focus on malware code, behavioral analysis focuses on the “symptoms” of malware infection. When network traffic indicates unexpected behavior, it may not be clear at first what is causing the change in behavior. However, there are known indicators that a piece of software may be malicious, for example when it attempts to gain elevated privileges or interacts in an anomalous manner with other software or files on a system. Often, behavioral analysis is analogized to the medical profession: a doctor can often tell when someone is sick even before knowing exactly what the problem is. Behavioral analysis complements other types of analysis by discovering unknown threats that have not yet been identified and therefore have no known signatures.<sup>109</sup>

**Advanced Capabilities:** Providers can use algorithms to detect anomalous traffic patterns and leverage institutional knowledge or if necessary hire external security experts to diagnose the underlying causes of the anomalous traffic.

### *d. Packet sampling*

To make sense of the enormous amounts of data flowing through a network, many leading providers use a technique called packet sampling. This technique involves developing rich views of traffic flow from samples of network traffic captured by routers. By reducing the amount of data that needs to be inspected, packet sampling allows operators of large networks to analyze traffic, even as the size and speed of modern networks increases.

**Baseline Practices:** Providers should at least sample packets at pseudorandom<sup>†</sup>, giving packets a chance of being selected for inspection. This sampling may be performed on a content-neutral basis.

**Advanced Capabilities:** Providers can make use of more complex sampling techniques that weigh probability and adapt responsively to traffic changes. Providers may inspect for specific content associated with malware threats.

<sup>†</sup> “Pseudorandom” numbers or processes have similarly unpredictable characteristics to truly random numbers or processes, but aren’t actually mathematically random or unpredictable. In systems without means to generate true randomness, pseudorandomness is used.

### e. Honeypots and data level decoys

In addition to network level solutions described above, providers may make use of data level decoys such as honeypots to “bait” attackers. A honeypot is typically data or a system within a network that appears to be of value to malicious actors, who are then blocked or monitored when they attempt to access it. It is worth noting that honeypots and other decoys can be deployed by third parties, and providers may work with such entities to discover potential criminal activity or other cyber-attacks. Due to their usefulness in discovering criminal activity, honeypots are used in law enforcement sting operations.

**Baseline Practices:** Providers can deploy a low interaction honeypot, which has limited features and information-gathering capabilities but is low-risk because no actual intrusion takes place. The honeypot simulates a successful intrusion to fool attackers and collect information about them.

**Advanced Capabilities:** Providers can learn more about attackers by deploying a high interaction honeypot. Under this scenario, an attacker interacts with the provider’s actual system rather than an imitation, often exposing previously unknown attack vectors. Due to increased exposure to attacks, high interaction honeypots are inherently riskier, but also more revealing of attackers’ methods.

## 2. MITIGATE AGAINST DISTRIBUTED THREATS

Given detection of malicious traffic and potential threats, infrastructure providers can also apply a variety of mitigation methods, described below, to address these challenges.

**Summary of Baseline Mitigation Practices:** Providers should use ingress filtering — that is, apply a filter that can limit the rate of inbound traffic. Providers should also make a reasonable effort to shape traffic on their networks and use blackholing and sinkholing as network management tools.

**Summary of Advanced Mitigation Capabilities:** Companies with access to greater resources may use egress filtering in addition to ingress filtering, thereby limiting the rate of both outbound and inbound traffic. They may use access control lists (ACLs) to reduce attack vectors. Companies may take steps to minimize service disruptions when shaping traffic, for example by deploying selective black holes. They may use technologies such as BGP flowspec to increase traffic management options. They are able to work in partnership with government and industry to take down malicious botnets. They may also offer commercial services such as scrubbing traffic and DDoS protection.

### a. Filtering

One of the complications when mitigating botnets is that malicious actors use IP-spoofing to make bad traffic appear to come from somewhere other than its actual place of origin.<sup>110</sup> By filtering out bad traffic as it enters the provider’s network (i.e. ingress filtering, BCP38 and BCP84),<sup>111</sup> providers can reduce the effectiveness of spoofing and therefore make DDoS attacks more difficult to carry out. Due to the readily observable benefits of this practice, the Internet Engineering Task Force (IETF) has recognized ingress filtering as a best practice.<sup>112</sup> It is worth noting that ingress filtering works better at network ingress points such as customer premises, whereas it is much more difficult at network exchange points.



Moreover, while providers are often well-situated to filter malicious traffic, techniques such as BCP38 should be employed by any entity that is operating its own IP address space, including enterprises. Providers such as ISPs allocate many IP addresses to their clients who in turn may operate their own filtering capabilities and also need to follow BCP38.

Additionally, by deploying filters at the edge of their networks, providers can monitor the traffic coming out of, or egressing from, their corners of the ecosystem and reduce harm to other parties. Egress filtering is not a replacement for ingress filtering but rather a complementary solution. A combination of ingress and egress filtering is the best way for providers to increase resilience.<sup>113</sup>

Finally, in a network setting, ACLs are used to identify traffic flows based on parameters such as its source and destination, IP protocol, ports, EtherType, and other characteristics. A common example is that traffic from a lower security interface cannot access a higher security interface.<sup>114</sup> In some contexts, ACLs may be configured to account for the access privileges of individual users to further limit the attack vectors by which malware can infiltrate a network.

**Baseline Practices:** Providers should filter inbound traffic (ingress filtering) at network ingress points to reduce the amount of malicious traffic that enters their networks. The filter should be able to limit the rate of inbound traffic in the event of an attack that could overwhelm network resources.

**Advanced Capabilities:** Ideally, providers should filter outbound traffic (egress filtering) in addition to inbound traffic, and they should be able to limit the rate of traffic regardless of whether it is outbound or inbound. This hybrid solution provides a greater amount of protection and makes providers responsible neighbors to others in the ecosystem. Additionally, providers can use ACLs to reduce attack vectors.

### ***b. Traffic shaping***

When potentially malicious traffic is identified, providers can securely manage traffic either by using techniques that will typically result in the traffic being dropped or by delaying traffic when the data rate is anomalously high. Both of these techniques can be useful in specific circumstances and may be part of a comprehensive traffic management strategy.<sup>115</sup>

**Baseline Practices:** Providers should make a reasonable effort to shape traffic on their networks. At a minimum, providers should be able to deploy a “black hole” that prevents traffic from reaching a target. Efforts should be made to reduce disruptions to legitimate services by redirecting traffic or dropping traffic only within defined geographic regions.

**Advanced Capabilities:** Providers with more resources can shape traffic without causing as many disruptions to legitimate traffic. For example, commercial scrubbing centers can clean-up traffic by filtering out the malicious elements and sending legitimate traffic to its destination. Small providers may form partnerships with large providers to offer these services to their customers.

### c. Blackholing

Blackholing is a technique that drops all traffic headed toward a specific online destination. A common version of this technique is remotely triggered destination based blackholing (RTDBH) in which upstream networks, which are typically closest to the attack source, drop the malicious traffic before it reaches a potential victim.

Although blackholing is effective at preventing malicious traffic from reaching its destination, an obvious drawback is that legitimate traffic cannot reach the destination either, which may be the explicit goal of malicious actors. To minimize this problem, providers may employ a technique known as selective blackholing, which drops traffic from chosen geographic regions (such as a country or continent) while allowing traffic from other regions to reach its destination.

**Baseline Practices:** Providers should make use of blackholing to protect their networks. While ideally providers should minimize disruptions to legitimate traffic, they should at least deploy the basic RTDBH in circumstances where more granular tools are not available or would not work as well.

**Advanced Capabilities:** Providers can improve the effectiveness of blackholing by leveraging partnerships with other providers both for sensors and filtering points of presence. Moreover, providers can deploy selective black holes that minimize disruptions to legitimate traffic by targeting a specific geographic region.

### d. Sinkholing

Sinkholing is a technique where traffic within a particular IP-range is sent to a designated server (the “sinkhole”) whereas traffic outside that IP-range continues as normal. The purpose of sinkholing is to capture botnets for both research and mitigation purposes.<sup>116</sup> Sinkholing is often accomplished through policy routing or other routing methods, which trap the malware that makes up a botnet in the sinkhole, where it can be studied by law enforcement and researchers. When malware caught in a sinkhole tries to communicate with command-and-control servers, security experts can track the IP addresses of machines the malware feeds information to, thus gaining insight into criminal activities. Providers can also completely sever communications between the malware and the command-and-control servers. Sinkholes are essential to large-scale takedowns of botnets, which use hundreds of thousands of internet-enabled systems in multiple countries throughout the world.

**Baseline Practices:** Providers should use sinkholing as a network management tool to redirect inbound malicious traffic and to collect information about threats to a provider’s network for analysis or information-sharing.

**Advanced Capabilities:** Industry leaders can use sinkholes to disrupt and gather intelligence on ecosystem-wide threats in partnership with other providers and law enforcement. Providers can also assist international law enforcement operations by coordinating effectively with authorities and stakeholders across numerous jurisdictions.

#### *e. Scrubbing*

Scrubbing solutions are typically implemented by dedicated scrubbing centers, which analyze network traffic and cleanse it of malicious traffic, including DDoS. Because scrubbing is resource-intensive compared to other solutions, several large providers offer scrubbing as a commercial service. By redirecting traffic to the centers instead of dropping it, scrubbing allows legitimate traffic to reach its destination with a high degree of success. This makes scrubbing a preferable alternative to blackholing and sinkholing for many enterprises.

**Advanced Capabilities:** Scrubbing centers can add an important layer of protection to a provider or customer's defenses by filtering many types of attacks, not limited merely to volumetric flood attacks. For example, the centers may integrate technology that protects against SSL (encrypted links) based attacks.

#### *f. BGP flowspec*

Border Gateway Protocol (BGP) flow specification (flowspec) is a dynamic technology that enables providers to rapidly deploy a variety of different mitigation options, thereby allowing experts to make judgment calls on a situational basis. Unlike routers that only support blackholing, flowspec routers allow additional options such as sinkholing traffic so it can be studied by experts or, alternatively, shaping traffic and allowing it to proceed at a defined rate.<sup>117</sup>

**Advanced Capabilities:** Providers can use BGP flowspec to develop custom instructions for border routers instead of traditional one-size-fits all solutions. With BGP flowspec, routers can be instructed to either drop traffic, reroute the traffic, or limit the rate of traffic under appropriate validation of the flowspec originator.

### 3. COORDINATE WITH CUSTOMERS AND PEERS

Remediating botnets or other distributed threats may require providers to notify their customers or peers about a development to secure their cooperation. Obviously, the effectiveness of user-notifications hinges largely on the user. A study commissioned by M3AAWG found that telephone calls and postal mail are the most effective ways to get in contact with users.<sup>118</sup> Other available methods, which can and should be used, include email and webpage notices. Another method of contacting users is the “walled garden” — this approach limits user access to online services until they take specific steps determined by their provider. In some countries, approaches of this later kind raise legal or public policy concerns.<sup>119</sup> Peers can be notified with many of the same methods as customers. The notifications will be more effective if there is an established relationship. It is useful for providers to build familiarity with key players in their industries so that introductions do not have to be made for the first time during an emergency.

**Baseline Practices:** Providers should notify customers or peers who violate the acceptable use policy or engage in nefarious activities. If traffic from a customer or peer is blocked, provide both (1) a text or phone message *and* (2) email/user account webpage notice. The customer or peer should be provided with clear instructions on how to contact the provider via communications channels that are not being blocked.

**Advanced Capabilities:** Providers with trained staff and dedicated resources can greatly reduce the false positive rate so that customers rarely experience interruption when using services in a legitimate manner.

### 4. ADDRESS DOMAIN SEIZURE AND TAKEDOWN

Law enforcement has specific tools available that have been used in recent years to successfully mitigate malicious botnets and criminal actors with some success. Where good evidence exists that a criminal network is using particular domains to carry out their nefarious purposes (e.g., botnet attacks), a provider may work in cooperation with — and usually at the mandatory direction of — law enforcement to take down the domains, in accordance with relevant laws. Law enforcement action that leads to real-world consequences for malicious actors is the only solution that deals with the cause of botnets and DDoS attacks, rather than the symptoms. Law enforcement action of this kind is resource-intensive and often requires extensive forensic analysis. Large-scale domain seizures may also require international coordinated efforts.<sup>120</sup> For example, in 2016, providers worked with government officials from more than 30 countries to take down the Avalanche botnet and seize control of more than 800,000 domains scattered throughout the global internet and communications ecosystem.<sup>121</sup>

**Baseline Practices:** Providers should maintain an easy-to-find list of points of contact for law enforcement and security researchers. Providers should also have a well-defined policy describing how they can and cannot support law enforcement efforts.

**Advanced Capabilities:** Generally, industry leaders will have more procedures and technologies with which to support law enforcement. They will also have defined policies and legal positions on specific law enforcement tactics. They may conduct global risk assessment to account for global legal requirements. In addition to cooperating with law enforcement, providers may have processes for collaborating with competitors during exceptional events.

## B. SOFTWARE DEVELOPMENT

Software is an increasingly ubiquitous element of every other component of the ecosystem addressed in this Guide. As discussed throughout this Guide, there are a wide variety of complex development processes and interdependencies that drive software innovation and improvement in the major systemic users of software highlighted in the Guide: Infrastructure, IoT Devices, Systems Installers, and Enterprises. Accordingly, this section does not seek to capture the various baseline security practices and advanced capabilities that are pertinent to specialized software development in each part of the ecosystem. Instead, it aims to underscore the vital importance of secure software throughout and in all parts of that ecosystem. When not addressed specifically elsewhere in this Guide, software development should generally consist of these practices.

### Baseline Practices and Advanced Capabilities for Software

#### 1. SECURE-BY-DESIGN DEVELOPMENT PRACTICES

Software and applications are increasingly integrated into our commercial and infrastructure processes and products to improve efficiencies. But this makes them a prime target for hackers. The global economy, critical infrastructure and government operations have increased their dependence on software.

Organizations that follow best practices make security an element of quality, conducting a range of secure development practices, including developer training, static application security scanning, threat modeling, dynamic application security testing, and manual penetration testing throughout the development lifecycle on a risk management basis. Resources to help developers adopt these best practices are publicly available. For instance, SAFECode (the Software Assurance Forum for Excellence in Code), a leading organization dedicated to promoting software assurance, publishes secure software development training resources available for free to the public, including the *Fundamental Practices for Secure Software Development*.<sup>122</sup>

**Baseline Practices:** Secure-by-design development should include the following at a minimum:

- ▶ **Strong encryption of data at rest and in transit:** Encryption inhibits the visibility of data in the event that it is stolen or improperly accessed. Whether the data is resting (i.e. stored) or in transit, encryption is an essential tool to protect information. While there are different encryption options suited to the needs of specific organizations and products, the encryption should generally use a strong algorithm that cannot be broken easily in the context of its particular use case. The strength of an algorithm may vary contextually, depending on factors such as the type of attack at issue and the need for certain kinds of services to function properly. For example, strong encryption may prevent most firewalls and other security packet inspection services from working.
- ▶ **Security by default:** The default configuration settings of software should place a high emphasis on security. The settings should have to be deliberately changed in order for the software to lower its defenses to allow for more options. This principle reduces the attack vectors that malicious actors can exploit significantly.



- ▶ *Patchability and design for updating:* Software should be designed with the expectation that patches and updates will be necessary to protect against malicious actors' constantly evolving and increasingly sophisticated attacks. Patches and updates should be deliverable with minimal manual intervention in a reasonably quick and secure manner to systems with the software installed.
- ▶ *Principle of least privilege:* By limiting user and application access to only the essential privileges needed to perform necessary tasks, software developers can reduce the attack surface of a product. Applying the principle of least privilege in the design phase reduces the chance that a malicious actor or compromised service will gain administrative access and control over a system.
- ▶ *Software composition analysis:* The purpose of this analysis is to create an inventory of open source and other third-party components in the product. In doing so, software developers can maintain awareness of components they did not develop themselves in case problems arise, even if they cannot guarantee the security of third-party and open source components. Having an inventory of what components are used in products and applications can also help development organizations track and identify associated known vulnerabilities.
- ▶ *Software security awareness and education:* Awareness-raising should extend to all personnel who are part of the software development process, including developers, product managers and others. Cost-effective educational opportunities or training exercises should be made available.

**Advanced Capabilities:** Leading secure-by-design practices include the following:

- ▶ *Dynamic application security testing (DAST):* This advanced technology uses penetration testing (a simulated attack) to discover vulnerabilities while an application is running. This kind of testing can be especially useful in the IoT context. However, it requires manageable configuration options and the ability to hire highly skilled specialists.
- ▶ *Static application security testing (SAST):* With this advanced technology, developers can scan source code or binaries and identify vulnerabilities. It is limited to supported languages and platforms. For many products in the IoT space, this might not be an option. However, careful peer code review of especially sensitive components may be used to increase security.
- ▶ *Threat modeling and analysis of risks to architecture:* Companies that work with governments or whose operations are highly sensitive may hire teams of experts to determine how malicious actors would hypothetically create or exploit vulnerabilities in a system to achieve nefarious ends. A threat model may consider many types of risks, including those involving automated, distributed attacks.
- ▶ *Security-focused toolchains:* Developers may make use of security-focused toolchains to create new software. A toolchain is a collection of software or hardware tools that facilitate software development. When toolchains prioritize security, coding errors are less frequent and providers can enforce quality controls. Companies may integrate new vulnerabilities and lessons learned into development tools.
- ▶ *Secure third-party and open source components:* Leading companies will ensure third-party components and open source libraries being used are free of known vulnerabilities.
- ▶ Additionally, companies may provide attestation to customers about elements of secure software development process and seek certification of alignment with international standards.

## 2. SECURITY VULNERABILITY MANAGEMENT

Different companies throughout the world have different policies with regard to when and for how long security patches are available to customers after a product ships in order to remediate newly discovered vulnerabilities. While major product manufacturers tend to release patches for their products more regularly, smaller manufacturers are generally less likely to devote sufficient resources to developing and making available security patches.<sup>123</sup>

**Baseline Practices:** Providers should prioritize critical vulnerabilities in mission critical applications.

**Advanced Capabilities:** More advanced providers can fix nearly all known vulnerabilities, especially those prioritized during risk assessment. They have the ability to provide security assurance to those purchasing software from their company or interacting with their company through applications.

## 3. TRANSPARENCY OF SECURE DEVELOPMENT PROCESSES

Each of the above practices plays an important role in the development of secure software and hardware. Software development organizations and the private sector have initiated the development of market-based assessments of secure development processes.<sup>124</sup> However, a framework developed in partnership between government and industry stakeholders could help standardize terminology and processes, building stronger market confidence. NIST is currently partnering with SAFECode and other stakeholders to develop a special publication on secure software development processes and practices. NTIA is convening a multistakeholder process to explore how organizations can communicate information about third-party software components and offer greater transparency.<sup>125</sup>

**Baseline Practices:** Provide attestation of security posture to companies purchasing software.

**Advanced Capabilities:** Provide security assurance to those purchasing software from the company and interacting with the company through applications.

## C. IOT DEVICES

This 2020 edition of the Guide benefits from work done in the *C2 Consensus on IoT Device Security Baseline Capabilities*,<sup>126</sup> a related project hosted by the CSDE. The CSDE convened twenty major standards bodies, technical alliances and civil society groups to leverage the organizations' extensive cybersecurity expertise. The C2 Consensus white paper of recommended capabilities was published in September 2019.

In this 2020 update of the Guide, the CSDE reaffirms the practices in the 2018 Guide but reorganizes the material and rewords the guidance to align with the C2 Consensus and other industry efforts. Two additional practices are added to the 2018 guidance based on the results of the C2 Consensus (*Event Logging and Device Intent Documentation*).

## Baseline Practices and Advanced Capabilities for IoT Devices

### 1. SECURE DEVELOPMENT

Security must be integrated into the development process starting at the requirements planning and continuing through to qualification and release.<sup>127</sup> This section lists development practices that are important to IoT device security but not typically observable outside the organization.

#### a. Secure Development Lifecycle Process

In the SDL process, each development phase has security activities that can be done manually or automatically.<sup>128</sup>

**Baseline Practices:** A secure development lifecycle (SDL) process should be in place.

While specific elements of an SDL may vary, SDLs should include the following security-oriented elements: threat identification and disposition; coding standards; 3rd party software requirements; software security controls and capabilities test and validation; and new vulnerability identification and handling.

**Advanced Capabilities:** After establishing a secure development lifecycle process, the advanced company is measuring and growing process capabilities. Measuring SDL capabilities is part of the BSIMM project (Building Security In — Maturity Model<sup>129</sup>); the BSIMM materials are open source and can be a resource for this effort.

#### b. Security-Focused Toolchain Use

Security-Focused Toolchains are collections of software or hardware that not only enable development, production, and management of products, but also have been designed to enhance the security of the end product.

**Baseline Practices:** Tools that are able to check if the implementation is following secure coding guidelines and to search for a subset of known Common Vulnerabilities and Exposures (CVEs) should be used to develop, compile, build and maintain software. Memory-safe languages should also be used.

**Advanced Capabilities:** Testing techniques such as fuzzing, symbolic execution, sandboxing, static analysis and dynamic analysis should be used to supplement the security-focused tool chain, to find vulnerabilities during the development process.

### 2. SECURE CAPABILITIES

This section lists device capabilities that are typically observable properties of a device after shipping and installation. In some system architectures, these important device properties may be found not in the device itself, but in a gateway or hub that is part of the overall structure. When a device uses a particular wired or wireless technology, it will require a hub or gateway to interface to the general internet. The properties below may sometimes be located on the hub or gateway rather than on the device, and still be fully effective because there is no access to the device except via the hub or gateway.

#### *a. Device Identifiers*

The identity of a device plays a role throughout its entire lifecycle. Identifiers are used to onboard devices to a network(s), register, authenticate, authorize, assign access lists and policy, control and manage the device in the performance of services and applications. Identifiers can also help understand what happened after a device or network has been compromised.

**Baseline Practices:** The device should have a unique value associated with it that is distinct and distinguishes the device from all other devices.

**Advanced Capabilities:** The security of the device identifier should be strengthened by additional cryptographic protections for confidentiality, integrity and availability.

#### *b. Secured Access*

IoT products typically require local or remote administrative services. During product development and manufacturing there may be requirements for other kinds of low-level access to memory, processor, peripherals, or control flow that are not required or available to the end user of the device. These additional capabilities must be carefully protected.

**Baseline Practices:** The device must be carefully protected by requiring user authentication to read or modify the software, firmware and configuration, including means to ensure device-unique credentials for administrative access, and by protecting access to interfaces.

Typical steps at this level include: Unique “admin” credentials per device or a first-boot requirement to change passwords; rate-limiting techniques to prevent brute-force password guessing; securing or disabling developer-level ports and services prior to product shipment; removing unused or insecure local and remote administrative services such as telnet.

**Advanced Capabilities:** Multi-factor authentication user access control should be considered.

### c. *Data Is Protected*

This category is primarily about protecting stored data on the device and encrypting data communications. Implementing such protections may involve decisions regarding, e.g., secure hardware elements, secure boot process, etc.; see also the discussion on Cryptography with regard to the discussion on Hardware Rooted Security.

**Baseline Practices:** The confidentiality and integrity of data at rest and in transit should be protected. To that end, data communications should be encrypted except in cases where risk analysis indicates otherwise. Sensitive data should be stored encrypted.

In general, the security mechanisms available in whatever system is used should be employed to protect data at rest and in transit.

**Advanced Capabilities:** Up-to-date versions of protocols and security mechanisms should be carefully selected; note that the most recent version of a specification may not obsolete a prior version. The organization responsible for maintaining the relevant specification (for the protocol or security mechanism) should be used to determine version applicability.

Secure memory can be used in lieu of encryption for stored information. Encryption key methods comporting with NIST FIPS 140-2 or ISO/IEC 24759 should be used.<sup>130</sup>

### d. *Industry-Accepted Protocols*

Good cryptography is difficult. Cryptography that has been reviewed and tested by experts is much more likely to be successful. Industry-accepted protocols have gone through this process and have embedded expert experience.

**Baseline Practices:** Use of secure, widely used protocols, excluding deprecated and replaced versions and protocols, for communications to and from the device.

**Advanced Capabilities:** Secure memory can be used in lieu of encryption for stored information. Encryption key methods comporting with or equivalent to NIST FIPS 140-2 or ISO/IEC 24759 should be used.<sup>131</sup>



#### ***e. Data Validation***

Data that can be provided by an outside factor may be crafted to include special characters beyond basic alphanumeric characters. Characters like “.”, “\”, “%” and “:” may have consequences unintended by the developer. Malicious data strings are part of many exploits.

**Baseline Practices:** Any input received from outside the system must be managed so that an outside adversary cannot arrange for it to be used directly as code, commands, or other execution flow inputs. Input should be validated for length, character type, and acceptable values or ranges. Output from one subsystem to another or to another site should also be filtered.

**Advanced Capabilities:** Any data originating outside the device that will be processed internally is validated at the input and canonicalized at the output of each stage of processing internal to the device.

#### ***f. Event Logging***

Logging is important for forensic analysis and real time understanding of system failures. When something goes wrong, it is important to understand what chain of events led to a failure, and what devices are impacted. Logging to an external system is desirable but not always feasible.

**Baseline Practices:** Relevant cybersecurity events should be recorded (subject to available memory space), secured and available to authorized users. Relevant events are application-specific but examples include failed login attempts or negative results from cybersecurity checks such as boot time measurement or hash verification.

#### ***g. Cryptography***

**Baseline Practices:** Where cryptographic methods are used to ensure data integrity and confidentiality, rights authentication and non-repudiation of requests, they should be chosen to match the assessed risk. The implementation should use open, published, proven, and peer-reviewed cryptographic methods with appropriate parameter, algorithm and option selections.

Where feasible, cryptographic methods should be updateable.

Deprecated methods are to be avoided.

Hardware-rooted security should be considered as to how it fits into the secure development lifecycles of current and future products.

Device manufacturers should not rely solely on use of obfuscation to secure secrets (e.g., device keys, sensitive data), but obfuscation may be used to increase the difficulty of an attacker to locate the secret. Still, the secret should be protected by other means such as access control and encryption.

**Advanced Capabilities:** Strong, proven, updateable cryptography using open, peer-reviewed methods and algorithms. Ensure cryptography has the ability to support post-quantum resistant key lengths for symmetric encryption. Hardware-rooted security is utilized where technically feasible.

Regarding roots of trust, various types of attacks rely on imitating another entity. For example, a trusted source for new software for a device is generally the original hardware manufacturer. Installation of software corrupted with malware is obviously something to prevent. This begs the question of how to tell the difference.

The solution is to have a system of trust. A trust chain is a linkage of hardware and software elements in which each element is validated as it is added to the chain. At the beginning of the chain is a root of trust, which is provided by an authoritative entity. Validation is done cryptographically, using digital signatures. Because the first element ties back to a trusted authority, each element that is cryptographically validated by the chain can also be trusted.

When the system receives a signed software update, it can check the digital signature. Because the system itself is rooted in the trust of the original authoritative entity, after the software update is validated, the software can be trusted.

#### ***h. Patchability***

This capability can be quite difficult from a technical and feasibility point of view. However, no product can be considered perfectly secure from the point of manufacturing to the end of useful life. Until the device is taken offline or decommissioned, updates may be necessary to address newly-discovered exploits. Industry is offering solutions: Some companies offer IoT “platforms” that include remote software update.

**Baseline Practices:** A plan for secure updates with anti-rollback protection and proper access control throughout a defined security support period, where technically feasible.<sup>132</sup>

#### ***i. Reprovisioning***

The ability to revert a device to a known good “blank” state allows for removal of sensitive data from a device when it changes hands, such as in the sale of a house for smart home devices, or for recycling for all kinds of devices.

**Baseline Practices:** The manufacturer provides authorized users with the capability to securely reconfigure and redeploy a device post-market, especially to return the product to factory defaults or an authorized restore point, and securely remove data collected by the device (that is not essential to its operation), within a defined period established by the organization.

#### ***j. Device Intent Signaling***

For similar reasons as Device Intent Documentation (see below), the spread of botnets can be significantly reduced by protocols such as Manufacturer Usage Descriptor (MUD).<sup>133</sup> Other tools include OMA-DM<sup>134</sup> and TR-69<sup>135</sup> (the latter two being applicable in cases where the devices can be managed directly), security requirements including Open Connectivity Forum Security Profiles (Black, Blue and Purple), and proposals such as IoTSense.<sup>136</sup>

**Advanced Capabilities:** The device supports the process of authenticating the device, authorizing it with credentials, and configuring it to communicate within the appropriate security domain.

#### ***k. Device Network Onboarding***

If a device has access to the network, it should be authorized to that access. Unauthorized devices in home and enterprise environments create weaknesses in the security of the network. A secure and defined onboarding process reduces the inconvenience of attaching a device to the network and enables it to participate under authorization.

**Advanced Capabilities:** The device supports a protocol for the device to provide information to routers or firewalls upstream regarding the intended network usage. Equivalently, the device provides heuristics related to its own behavior in normal operation in support of network analysis.

### **3. PRODUCT LIFECYCLE MANAGEMENT**

Product Lifecycle Management (PLM) refers to actively managing a product from conception through design, manufacturing, support and end-of-life.

#### ***a. Vulnerability Handling***

Vulnerabilities happen. An organization should have active processes to find them, such as internal efforts, threat-sharing and openness to outside (ethical) disclosure.

**Baseline Practices:** Providers — manufacturers and retailers — should create a security vulnerability policy and process to identify, prioritize, mitigate, and where appropriate disclose known security vulnerabilities in their products.

#### ***b. EoL/EoS Updates and Disclosure***

This capability must be considered carefully within the organization. It is tied to vulnerability handling, the product lifecycle, terms of service and more.

**Baseline Practices:** Device providers should have a defined security support policy that includes the handling of any the end-of-life (EoL) or end-of-service (EoS) security vulnerabilities, whether updates will be made available and how, and what to do with the device at that time.

#### ***c. Device Intent Documentation***

A device's designed and intended network usage—ports, protocols, sites to be visited, expected data traffic levels, communications with other devices—is important information when determining if the unit has been compromised, including into a botnet.

**Baseline Practices:** The device manufacturer provides documentation of the device's as-designed network usage publicly, either in product documentation or other means for device users.

## D. HOME AND SMALL BUSINESS SYSTEMS INSTALLATION

Homes and small businesses benefit from connected devices in several categories. Heating, ventilation, and air conditioning (HVAC) systems are connected for smart features and remote access by the occupant. Security systems include cameras, locks, and alarm systems that can all be managed via the internet. Entertainment systems benefit from central controls so that complex audio and video configurations can be managed with ease. There is tremendous diversity of manufacturers and systems in these categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others.

Ideally, every device and system entering a home, office, retail, medical, or industrial environment will be secured by best practices in the entire lifecycle of the device. This lifecycle includes installation and configuration of the device. A good installation will achieve the “best available security” from the manufactured product. In this section are baseline practices and advanced capabilities for achieving that best available security from the most common device types.

The material below draws heavily from *The Connected Home Security System*.<sup>137</sup>

### Baseline Practices and Advanced Capabilities for Home and Small Business Systems Installation

#### 1. AUTHENTICATION AND CREDENTIAL MANAGEMENT

Installations can benefit from Password Management Systems, which are encrypted storage for passwords. These systems take the burden away from users of remembering and managing passwords and putting the passwords in a secure place.

**Baseline Practices:** If a password is not unique to the device, the installer should change to a strong password. (See [1], “Passwords”). Different passwords must be used for all devices and systems. The installation should use a trusted password management system.

**Advanced Capabilities:** Multi-factor authentication user access control is used.

#### 2. NETWORK CONFIGURATION

Network Configuration refers to the physical and logical layout and connections and settings of network components.

##### a. General

**Baseline Practices:** Systems (desktops, laptops, etc.) should have up-to-date anti-virus and anti-malware tools installed and running. No systems with administrative privileges should be running unless specifically required.

### ***b. Firewall, Access Point, and Router Configuration***

**Baseline Practices:** UPnP should be disabled on the WAN side (internet facing side) unless required for a legitimate purpose (e.g., peer-to-peer gaming). Adequate DHCP space should be allotted for expected usage but not exceed expected usage. A firewall should be enabled with only required ports unblocked. Port forwarding should be disabled except for specific applications where it is required.

**Advanced Capabilities:** Networks should be monitored, use non-standard port values on applications, and have port forwarding only selectively enabled for specific applications in conjunction with firewall protections. Although a sophisticated attacker can overcome it, MAC address filtering should still be used.

### ***c. Physical and Logical Structure***

**Baseline Practices:** Network access should be limited from outside the physical structure of the client site in terms of wireless power and physical wiring placement. Segments should be separated according to purpose and use separate physical or logical networks, using options such as separate radio channels, cabling, separate access points, or gateways.

**Advanced Capabilities:** Segments should additionally be separated for different purposes using VLANs or VPNs. A port scanning tool can be used to monitor the private network.

## **3. NETWORK HARDWARE MANAGEMENT**

Network Hardware Management refers to the ongoing process of keeping network devices properly identified and configured.

### ***a. Modems and Routers, Network Management Devices***

**Baseline Practices:** Networking devices should have a process or means for regularly updating firmware.

**Advanced Capabilities:** For ISP-provided modem/router/AP systems, a separate aftermarket router/AP can be added to handle LAN traffic for local control over software updates.

### ***b. Protocols***

Network Protocols are the multilevel languages devices used to communicate on networks, such as TCP, UDP, IP, RTP, etc.

**Baseline Practices:** Deprecated protocols should not be used. In particular, do not use or allow to be negotiated SSL (any version), or TLS 1.0 or 1.1.

**Advanced Capabilities:** Configure for the latest protocols where appropriate.



### c. *Wireless Links*

Wireless Links are radio-based network connections between devices. These links may be one way, bidirectional, or use a network topology among multiple devices.

#### 1) Bluetooth

**Baseline Practices:** Available security features should be enabled. “Non-discoverable” options should be used where available. No sensitive information should be exposed in Bluetooth low energy (BLE) beacon signals.

#### 2) NFC

**Baseline Practices:** NFC readers should not be situated or mounted to allow for easy “sniffing” or for easy tampering.

#### 3) Wi-Fi

**Baseline Practices:** In addition to the Baseline network configuration practices mentioned in other sections, up-to-date Wi-Fi encryption options should be used, such as WPA2 or WPA3 (the most recent version). WPS should be disabled. Neither default nor broadcast SSIDs should be used.

A “guest network” option is available on many Access Points; this should be enabled and made available for higher-risk users such as visitors or temporary residents/workers. If available, 802.11aw Management Frame protection should be enabled. Ensure the Access Point configuration access is protected with a strong password under the best practices described elsewhere in this document. Enable port filtering where appropriate. Choose an Access Point/Router with updatable firmware.

#### 4) Z-WAVE

**Baseline Practices:** Basic security involves unique Home IDs, password-protected administrative functions, and use of AES-128 enabled devices where available.

**Advanced Capabilities:** To increase security, RF power can meet the distance requirements and exclusively AES-128 enabled devices can be used.

#### 5) Zigbee

**Baseline Practices:** The only device connected to the internet should be the ZigBee gateway and there should be a firewall protecting it.

**Advanced Capabilities:** Internet traffic can be filtered when entering and leaving the ZigBee network by address (source and destination) and port number. Optional 802.15.4 security features can be enabled at the 802.15.4 level and at the network plus application level, where available.

#### 6) Remote Device Access Control

This category involves all kinds of remote access control of normal device functions such as security camera video, HVAC temperature control, vehicle subsystems such as remote start or door unlock, etc.

**Baseline Practices:** Alerts for device failure or tampering should be enabled when available. All remote access should be behind an IP restricted firewall, allowing only white-listed IP addresses and subnets to access the device, regardless of port. If remote access from outside the firewall is a required feature, VPNs and non-standard internet ports should be used for remote access.

### 4. SECURITY MAINTENANCE

**Baseline Practices:** Where possible, breach attempts on the network or other attempts on the installation should be tracked and reviewed for action. Breach attempts should be correlated to identify commonly attacked individuals or targets within the network. Network configuration should be documented, connected devices should be enumerated, and a security maintenance plan should be clearly defined.

## E. ENTERPRISES

As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, non-profit — have a critical role to play in securing the digital ecosystem.<sup>138</sup> While enterprises often are the victims of automated, distributed attacks as well as data exfiltration attempts, their vast systems also can be hijacked to increase the impact of DDoS and other distributed attacks on others. Accordingly, enterprises are collectively among the important stakeholders that share responsibility for adequately securing their networks and systems in order to help secure the broader digital ecosystem.

The millions of private sector and government enterprises worldwide differ considerably in terms of their technical knowledge and skills, access to resources, and incentives to adopt baseline security practices. Larger enterprises, for instance, often have a Chief Information Officer and a Chief Information Security Officer, each charged in part with securing the organization's networked systems and devices, including any IoT systems. Smaller enterprises may not have the resources for dedicated IT and information security personnel and instead rely on off-the-shelf solutions.

Organizations increasingly are developing and offering tools to help enterprises, both small and large, secure their networks and systems. Perhaps most relevant to this Guide is the effort by the Cybersecurity Coalition to develop and advance Profiles for DDoS and Botnet Prevention and Mitigation Profile under the Cybersecurity Framework,<sup>139</sup> intended to aid enterprises and other organizations in addressing and mitigating DDoS and other automated, distributed attacks.

Enterprises of all sizes also can take their own proactive steps to mitigate ecosystem risk through, for example, implementing appropriate identity and access management techniques and discontinuing the use of legacy and pirated products and software that do not receive updates, among other things. Steps like these can help enterprises protect sensitive data and intellectual property on their networks, in addition to helping to protect the ecosystem at large by reducing the attack surface for DDoS and other distributed attacks.

Of course, the suppliers and providers that developed this Guide are ourselves large global enterprises. Further, we provide high-end solutions to secure enterprise networks and mitigate against DDoS attacks and other automated, distributed threats. The “supply” side of this market is robust and growing; further development of the “demand” side of this market in terms of enterprises of all sizes requesting and negotiating for these services will bring further innovation, sophistication, and cost efficiencies in these services.

## Baseline Practices and Advanced Capabilities for Enterprises

### 1. SECURE UPDATES

While product manufacturers are responsible for creating secure updates, those updates generally do not install themselves without permission or other action by the user. The level of control organizations may need over updates varies considerably depending on the type of customer. A large enterprise or government agency with qualified staff, for example, can reasonably determine which kinds of security updates are appropriate and when to implement them. On the other hand, regular home users may benefit most from automatic updates.<sup>140</sup>

**Baseline Practices:** Enterprises should install updates as soon as they become available. Generally, automatic updates are preferable.

**Advanced Capabilities:** Enterprises with qualified technical staff can make informed determinations about the implementation of security updates.

### 2. REAL-TIME INFORMATION SHARING

Enterprises with large networks or highly sensitive networks (e.g., large enterprises and government agencies) can share critical threat information with other relevant stakeholders and ecosystem participants. These efforts have improved significantly in recent years and constitute a big step forward toward combating the threat of botnets and other automated, distributed threats.<sup>141</sup>

**Baseline Practices:** Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information. Examples include information from government and law enforcement information sharing activities, various CERTs, industry groups, network providers, RFC2142 addresses, and updates and alerts from vendors and other sources.

Enterprises should subscribe to multiple threat intelligence feeds or services to utilize in conjunction with security information and event management (SIEM) correlation/automation efforts. Enterprises should have processes in place to share threat information gained internally or externally with internal shareholders in a timely and actionable manner. Enterprises should maintain contact with sharing communities and be aware of the processes and safeguards to properly report/share cyber security incidents within their region and industry. Enterprises should conduct internal threat intelligence sharing on an ongoing basis. Indicators of compromise (IOCs) and notable threats should be shared on a regular cadence.

**Advanced Capabilities:** Advanced enterprises should be committed to enhancing the cyber threat information sharing community through the responsible and timely sharing of desensitized cyber threat information with the various appropriate sharing communities (government, industry, etc.). Advanced enterprises should ensure that they have sufficient capabilities to detect, analyze, and capture cyber threat information in formats that are conducive to sharing activities. Advanced enterprises should actively participate in the governance and enhancement of cyber threat information sharing communities appropriate to their region and industry. Advanced enterprises should seek to continuously improve their capabilities in detection, analysis, response, and sharing.

### 3. NETWORK ARCHITECTURES THAT SECURELY MANAGE TRAFFIC FLOWS

Enterprises can exercise control over the design of their network architectures to limit the flow of malicious traffic during a DDoS attack carried out using botnets or other means.<sup>142</sup> A network architecture designed with security as an explicit goal can complement other precautionary measures, such as anti-DDoS services offered by infrastructure providers and other ecosystem participants. Application Programming Interfaces (APIs) manage the connections between applications, devices, and back-end data systems. Broadly speaking, APIs make it possible for enterprises to open their back-end data and functionality for reuse in new application services. Deploying security at the perimeter, through an API Gateway, can help enterprises stop threats before they penetrate the enterprise, allowing them to provide access to enterprise data for application developers while maintaining strong security.

**Baseline Practices:** Enterprises should obtain intranet defense against DDoS by consuming capabilities and services provided by network service providers. Enterprises should standardize the internet to intranet interconnect architecture, operational policy and processes, access and packet flow control configuration settings. Enterprises should implement a regime that ensures this architecture is correctly deployed and operated. In addition, enterprises should inspect all inbound and outbound data flows and email and block packets or emails with malware; block unauthorized network traffic into the intranet; and utilize industry standard DMZ architecture and operational practices.

**Advanced Capabilities:** Advanced enterprises may identify observable behaviors that indicate botnet flows, such as botnet C&C flows, fastflux DNS, and accessing suspicious URLs. Advanced enterprises may automatically block botnet flows and remediate the sources of the flows; remove internet accessible URL links from inbound emails; share and receive information that is used to identify botnet actors; and prevent improper DNS actions by both the DNS requester and the DNS server.

To increase resiliency against distributed attacks, advanced enterprises may make use of Application Programming Interface Gateways. Application Programming Interfaces (APIs) manage the connections between applications, devices and back-end data systems. Deploying security in a centralized architecture through an API Gateway can help organizations provide access to enterprise data for application developers while maintaining strong security.

#### 4. ENHANCED DDOS RESILIENCE

Even with very successful customer awareness and educational outreach efforts, many customers will lack the technical expertise required to secure their own networks. Rather than ignoring the threat that botnets and other distributed attacks may pose, enterprises should purchase commercial DDoS protection suitable to their risk profile.<sup>143</sup> Commercial services may include off-premise protection or a combination of off-premise and on-premise protection that more robustly secures the enterprise against distributed attacks. When customers purchase commercial products and services, they substantially decrease the threat of botnets and other distributed attacks.

The CSDE's members provide some of the highest-end commercial DDoS solutions on the market. Examples include home gateways with integrated security, Anycast services, and a variety of managed security services. Anycast services increase resilience to DDoS attacks by providing multiple routes for content delivery and balancing workloads across multiple network elements, which may be spread throughout the world. If a DDoS attack compromises certain parts of a network, traffic is rerouted automatically to another part. Managed security services include commercial scrubbing services.<sup>144</sup> Other commercial services include network-based firewalls, mobile device management systems, threat analysis and event detection, secure VPN connectivity to the cloud, web and application security, and email security.

Providers may offer filtering solutions tailored to the unique needs and risk profiles of their customers. Ideally, these solutions will integrate both off-premise and on-premise defenses. Commercial services may allow malicious traffic to be blocked closer to the attack source, creating an extra layer of security for customers.

**Baseline Practices:** Enterprises should have capable retained/contingency support available to them to effectively respond to cyber security incidents and maintain a reasonable level of security. Enterprises should select commercial providers whose products and services include appropriate security capabilities (i.e., ISPs and cloud/hosting providers who have DDoS protection capabilities, software with auto-update capabilities, etc.). Enterprises should have documented, tested plans for incident response, including DDoS and botnet response. Enterprises should select commercial providers who can provide automated or default-on response. Enterprises should regularly re-evaluate the effectiveness of the commercial providers.

**Advanced Capabilities:** Advanced enterprises should take a multi-layered approach to DDoS and botnet protection that includes well-supported on and off-premise capabilities. Advanced enterprises should proactively increase their staff's technical expertise, determine gaps in this expertise, and address these gaps with appropriate training, retained/contingency support, and additional staff. Advanced enterprises should consider commercial services and software that offer advanced capabilities such as machine learning and pattern analysis to enable higher quality results. Advanced enterprises should seek to continuously improve their capabilities by regularly re-evaluating the capabilities available in the marketplace.



## 5. IDENTITY AND ACCESS MANAGEMENT

Identities constitute the unifying control point across applications, devices, data, and users. Identity and access management tools authenticate individuals and services and govern the actions they are permitted to take. One of the most important areas of IT risk relates to privileged users, such as IT Administrators, CISOs, and other individuals with enhanced systems access. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. Systems should be set up for administrators to only perform those actions that are essential for their role — enabling “least privileged access” for reduced risk. Threat analytics can provide insight on activity and work to prevent or flag anything unusual that indicates security risk.<sup>145</sup>

A recent development worth noting is the use of physical security keys instead of passwords or one-time codes. Since early 2017, when Google began requiring all of its employees — more than 85,000 in total — to use physical security keys, not a single employee’s work-related account has been phished.<sup>146</sup>

**Baseline Practices:** The identity and access management practices of organizations should at least include the following:

- ▶ *Authentication* (including multi-factor and risk-based authentication) — a time of access operation that assures that the subject is in fact the real subject and not an impersonator;
- ▶ *Authorization* — a time of access operation that determines, given the current state, whether access should be granted;
- ▶ *Access Governance* — a process for helping business leaders define and refine policies for determining appropriate access;
- ▶ *Accounting* — a process for logging data about the activity of individual users who access system resources to analyze trends and identify suspicious behavior;
- ▶ *Provisioning/Orchestration* — a set of operations that happens at times of change facilitating the join/move/leave process and the coordination of change events between disparate connected resources; and
- ▶ *Identity Repository* — a persistent store for maintaining the current state and attribute values of subjects’ profiles.

Enterprises should also adopt the practice of offboarding, which is the timely removal of identity from enterprise directory and revocation of identity and associated accesses, within 24 hours for privileged accesses and accesses to cloud resources.

To improve authentication, enterprises should use stronger and easier-to-remember passphrases instead of syntax rule-based passwords; check against a password dictionary; and use a password strength meter. Moreover, enterprises should make use of second or Multi-Factor Authentication (2FA/MFA) for privileged accesses, e.g., System Administrators. Organizations should use a centralized authentication service for web and SaaS applications with Single Sign-on which requires 2FA — step-up authentication — for devices that are not previously vetted and trusted. Moreover, enterprises should use FIDO U2F tokens to thwart phishing attacks or take other reasonable precautions to reduce the risk posed by phishing attacks.

Enterprises should adhere to the principle of least privileged access — access request based on roles via Role-Based Access Control (RBAC) and/or approvals, detection, and remediation of out-of-process, outlier, dormant, and Separation of Duties (SoD) violation accesses, and accesses governance via periodical revalidation of accesses (Continued Business Needs or CBN).

Enterprises should conduct privileged user monitoring and audit and Secure Information Event Management (SIEM). They should also have a credential/secret vault for service or application IDs — the IDs should not be stored in configuration files in plain-text.

**Advanced Capabilities:** Advanced enterprises may have more sophisticated methods of managing identity and access:

- ▶ *Continuous authentication* methods leverage behavioral and biometrics monitoring throughout a user session to determine if the session has been compromised.
- ▶ *Risk-based authentication* provides enterprises with a better understanding of the context around identity, such as through geo-location data or purchasing behavior. A system may recognize the identity, determine that traditional authentication is unnecessary, and allow access. Conversely, if the system detects anomalies, such as logging in from a foreign country in the middle of the night after having a few failed passwords, then this is a very high-risk operation and access will be denied absent additional authentication steps.
- ▶ *Privileged Access Management* solutions provide the visibility, monitoring and control needed for those users and accounts that have the “keys to the kingdom.” It is essential that administrators be allowed to perform only those actions that are essential for their role — enabling “least privileged access” for reduced risk. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.
- ▶ *Adaptive authentication* uses 2FA/MFA, with more complete and sophisticated risk calculation, above and beyond device fingerprinting, incorporating factors like intranet or internet, simultaneous access from multiple locations or geographies, logging-in at very odd hours, etc.
- ▶ *Closed-loop identity* governance integrates user activity monitoring and analytics on servers and inside applications with access management tools, e.g., revoke a privileged user’s access if he/she is detected of accessing protected data on server or inside applications in an unauthorized manner.
- ▶ *Smarter access* governance can be achieved with analytics and AI, e.g., detecting and revoking dormant accesses — accesses that have not been used by their owners for a prolonged period, signaling potential lapses in access governance or offboarding.
- ▶ *Detection of and safeguarding against hacking* can be improved with integration of privilege access management and User and Entity Behavior Analytics (UEBA): malware dropped onto workstations via spear phishing using social network info and emails will behave differently and can indicate that a workstation and privileged credentials have been compromised.

## 6. MITIGATING ISSUES WITH OUT-OF-DATE AND PIRATED PRODUCTS

Enterprises should discontinue use of the legacy products for which manufacturer support has ended.<sup>147</sup> A closely related problem from a technical support standpoint is pirated software. In the U.S., almost one in five personal computers run pirated software, whereas in China the percent of personal computers with pirated software often exceeds 70%.<sup>148</sup> Of course, manufacturers do not normally patch pirated software, which means it remains vulnerable to known exploits.<sup>149</sup> Enterprises should avoid pirated software and decrease the total number of vulnerabilities in the global internet and communications ecosystem.

**Baseline Practices:** Enterprises should replace legitimate supported products before manufacturer support expires. Enterprises should always avoid pirated products. Such products are illegal in most countries and they are also major contributors to security vulnerabilities throughout the ecosystem.<sup>150</sup>

**Advanced Capabilities:** Advanced enterprises may have the latest supported products available with the most up-to-date security features and capabilities.

## 06 / Next Steps and Conclusion

Publication of the 2020 version of this Guide constitutes the continuation of an unprecedented industry-led strategic campaign against botnets and other automated, distributed threats. The CSDE, USTelecom, and CTA urge stakeholders to implement the recommended practices to address the common challenges and turn the tide against bad actors.

As noted in the Introduction, the digital economy has been an engine for commercial growth and quality-of-life improvements across the world. No single stakeholder — in the public or private sector — controls this system, so securely managing the opportunities presented by this growth is the imperative responsibility of every stakeholder in the ICT community.

To that end, we set forth these baseline practices and advanced capabilities for the consideration of all stakeholders. These are dynamic, flexible solutions that are informed by voluntary consensus standards and driven by powerful market forces, and they can be implemented by stakeholders throughout the global digital economy. This is the best answer to the systemic cybersecurity challenges we face.

With this imperative in mind, we plan to continue updating, publishing and promoting a new version of this Guide on an annual basis, reflecting the latest developments and technological breakthroughs that will aid our companies and other companies throughout the world to drive observable and measurable security improvements — not only within their own networks and systems but also throughout the broader ecosystem.

For instance, while the hallmark of this year's efforts to combat botnets is IoT device security, based on the urgent need for a widely accepted baseline, not all significant botnets target connected devices — in fact, some of the world's most destructive botnets do not target connected devices at all. So, while it is clear that the future of botnets is closely intertwined with the future of IoT security, and the CSDE will continue to lead on this front, we will also explore other ways that botnets and other distributed threats can be reduced dramatically through our members' leadership. In recognizing the complex and layered nature of the botnet threat, the companies in the CSDE will engage these threats on multiple fronts.

More immediately, our next steps in the coming months is to engage with a broad spectrum of national and international stakeholders in the internet and communications ecosystem who are well positioned both to promote the recommended practices and further constructive engagement. The shared responsibility assumed by these diverse stakeholders is the key to securing the future of our digital economy.

## 07 / Contributing Organizations

### About CSDE

The Council to Secure the Digital Economy (CSDE) brings together companies from across the information and communications technology (ICT) sector to combat increasingly sophisticated and emerging cyber threats through collaborative actions. Founding partners include Akamai, AT&T, CA Technologies, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefonica and Verizon. CSDE is coordinated by USTelecom and the Consumer Technology Association (CTA).

### About USTelecom

USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives — all providing advanced communications service to both urban and rural markets.

### About the Consumer Technology Association

The Consumer Technology Association (CTA)<sup>TM</sup> is the trade association representing the \$377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies — 80 percent are small businesses and startups; others are among the world's best-known brands — enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® — the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.



## 08/Endnotes

- 1 Nat'l Inst. of Standards and Tech., NISTIR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (July 2019), <https://csrc.nist.gov/publications/detail/nistir/8259/draft>.
- 2 Malicious actors are also commonly referred to as hackers, although not all hackers are malicious. Generally this document uses the terms interchangeably, with the assumption that context will indicate whether the referenced individual is a malicious actor or not. It should also be noted that this document focuses on malicious actors, so generally speaking, "hacker" in this document is a malicious actor.
- 3 It is not practical to set requirements of all software types in the IoT ecosystem simultaneously. IoT Devices, Enterprises and Infrastructure have specific requirements. This section applies to areas not covered elsewhere in the Guide.
- 4 Heating, ventilation, and air conditioning (HVAC) systems are connected for smart features and remote access by the occupant. Security systems include cameras, locks, and alarm systems managed via the internet. Entertainment systems benefit from central controls so that complex audio and video configurations can be managed with ease. There is a tremendous diversity of manufacturers and systems in these categories. These systems can be installed by do-it-yourself home and business owners, or by professionals: integrators, alarm contractors, and others. Ideally, every Device System entering a home, office, retail, medical, or industrial environment will be secured by best practices in the entire lifecycle of the device — including installation and configuration of the device that achieves the "best available security" from the manufactured product.
- 5 Consumer Technology Association, *The Connected Home Security System*, <https://www.cta.tech/Membership/Member-Groups/Smart-Home-Division/Device-Security-Checklist.aspx> (last visited Oct. 10, 2018).
- 6 As major owners and users of networked devices and systems, including an exponentially increasing number of IoT device systems, enterprises of all kinds — government, private sector, academic, and non-profit — have a critical role to play in securing the digital ecosystem. While enterprises often are targets of automated, distributed attacks as well as data exfiltration attempts, their vast systems also can be hijacked to increase the impact of DDoS and other distributed attacks on others. Accordingly, enterprises are among the stakeholders that share responsibility for adequately securing their networks and systems in order to help secure the broader digital ecosystem. The millions of private sector and government enterprises worldwide differ considerably in terms of their technical knowledge and skills, access to resources, and incentives to adopt baseline security practices. Enterprises of all sizes can take their own proactive steps to mitigate ecosystem risk. Such steps can help enterprises protect sensitive data and intellectual property on their networks while also helping to protect the ecosystem at large by reducing the attack surface for botnets. The suppliers and providers that developed this Guide are large global enterprises, and we also provide high-end solutions to secure enterprise networks and mitigate against DDoS attacks and other automated, distributed threats. The "supply" side of this market is robust and growing, and further development of the "demand" side of this market in terms of enterprises of all sizes requesting and negotiating for these services will bring further innovation, sophistication, and cost efficiencies in these services.
- 7 Andrew Sheehy, *GDP Cannot Explain The Digital Economy*, Forbes (June 6, 2016), <https://www.forbes.com/sites/andrewsheehy/2016/06/06/gdp-cannot-explain-the-digital-economy/#47c4db1218db>.
- 8 Irving Wladawsky-Berger, *GDP Doesn't Work in a Digital Economy*, The Wall Street Journal (Nov. 3, 2017) <https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy>.
- 9 Paul Tentena, *Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025*, East African Business Week (May 30, 2018), <https://www.busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025/>.
- 10 See, e.g., Catalin Cimpanu, *Sly Malware Author Hides Cryptomining Botnet Behind Ever-shifting Proxy Service*, ZDNet (Sept. 13, 2018), <https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service/> ("[B]otnets focused on cryptocurrency mining operations have been one of the most active forms of malware infections in 2018.")
- 11 Sam Thielman and Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, The Guardian, (Oct. 21, 2016), <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service>.
- 12 Michael Newberg, *As Many as 48 Million Twitter Accounts Aren't People, Says Study*, CNBC (Mar. 10, 2017), <https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html>.
- 13 JP Buntinx, *Top 4 Largest Botnets to Date*, Null TX (Jan. 7, 2017), <https://themerkle.com/top-4-largest-botnets-to-date/>.
- 14 Daniel Newman, *The Top 8 IoT Trends for 2018*, Forbes (Dec. 19, 2017), <https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#48d7f78e67f72523096867f7> (citing HIS Markit IoT Trend Watch 2018, available at <https://ihsmarkit.com/industry/telecommunications.html>); see also Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>.
- 15 Jan-Peter Kleinhans, *Internet of Insecure Things: Can Security Assessment Cure Market Failures?*, Stiftung Neue Verantwortung (Dec. 2017), [https://www.stiftung-nv.de/sites/default/files/internet\\_of\\_insecure\\_things.pdf](https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf).
- 16 Bill Connor, *Ransomware-As-A-Service: The Next Great Cyber Threat?*, Forbes (Mar. 17, 2017), <https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#14a38e5b4123>.
- 17 Andy Greenberg, *The White House Blames Russia for NoPetya, the 'Most Costly Cyber Attack in History'*, Wired (Feb. 15, 2018) <https://www.wired.com/story/white-house-russia-notpetya-attribution/>; Damien Sharkov, *Russia Accused of 1.2 Billion NoPetya Cyberattack*, Newsweek (Feb. 15, 2018) <https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867>; CBS News, *What Can We Learn from the Most Devastating Cyber Attack in History?* (Aug. 22, 2018), <https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation> (discussing how NotPetya malware caused over \$10 billion in damage).

- 18 Alex Zaharov-Reutt, *Cyber Crime, Data Breaches to Cost Businesses US \$8 Trillion Thru 2022*, ITWire (April 25, 2017), [https://www.itwire.com/security/77782-\\$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html](https://www.itwire.com/security/77782-$8-trillion-business-cost-from-cybercrime-and-data-breaches-thru-2022.html).
- 19 Comm'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices 4* (Mar. 2015), available at [https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf) (acknowledging "the advantages of a nonregulatory approach over a prescriptive and static compliance regime").
- 20 Nat'l Inst. of Standards and Tech., NISTIR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (July 2019), <https://csrc.nist.gov/publications/detail/nistir/8259/draft>.
- 21 Daniel Palmer, *Researchers Discover Huge Crypto Scam Botnet on Twitter*, CoinDesk (Aug. 7, 2018), <https://www.coindesk.com/researchers-discover-huge-crypto-scam-botnet-on-twitter> ("Researchers have uncovered a huge botnet that mimics legitimate accounts on Twitter to spread a cryptocurrency "giveaway" scam.").
- 22 Charles DeBeck, Joshua Chung & Dave McMillen, *I Can't Believe Mirais: Tracking the Infamous IoT Malware*, SecurityIntelligence (July 18, 2019), <https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/>.
- 23 Charles DeBeck, Joshua Chung & Dave McMillen, *I Can't Believe Mirais: Tracking the Infamous IoT Malware*, SecurityIntelligence (July 18, 2019), <https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/>.
- 24 Mark Mayne, *New Mirai variant targets enterprises with 11 new exploits*, SC Media (Mar. 19, 2019), <https://www.scmagazineuk.com/new-mirai-variant-targets-enterprises-11-new-exploits/article/1579535>.
- 25 See SentinelOne, *Mirai Botnet Descendants Will Lead to Even Bigger Internet Outages*, CSO (Dec. 22, 2016), <https://www.csoonline.com/article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet-outages.html>.
- 26 Larry Cashdollar, *Latest Echobot: 26 Infection Vectors*, Akamai (June 13, 2019, 11:17 AM), <https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html>.
- 27 Charles DeBeck, Joshua Chung & Dave McMillen, *I Can't Believe Mirais: Tracking the Infamous IoT Malware*, SecurityIntelligence (July 18, 2019), <https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/>.
- 28 *2019 Threat Report*, CenturyLink 5-7, <https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf> (last visited Oct. 8, 2019).
- 29 *2019 Threat Report*, CenturyLink 5-7, <https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf> (last visited Oct. 8, 2019).
- 30 *2019 Threat Report*, CenturyLink 16, <https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf> (last visited Oct. 8, 2019).
- 31 Charles DeBeck, Joshua Chung & Dave McMillen, *I Can't Believe Mirais: Tracking the Infamous IoT Malware*, SecurityIntelligence (July 18, 2019), <https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/>.
- 32 Warick Ashford, *Phishing top security threat to business*, Computerweekly.com (Aug. 12, 2019, 4:00 PM), <https://www.computerweekly.com/news/252468231/Phishing-top-security-threat-to-business>.
- 33 *Incident Classification Patterns and Subsets*, Verizon, <https://enterprise.verizon.com/resources/reports/dbir/2019/incident-classification-patterns-subsets/> (last visited Oct. 8, 2019).
- 34 *A New Phase of TheMoon*, CenturyLink (Jan. 31, 2019), <https://blog.centurylink.com/a-new-phase-of-themoon/>.
- 35 Sergiu Gatlan, *Mirai Botnet Variants Targeting New Processors and Architectures*, BleepingComputer, (Apr. 9, 2019, 8:40 AM), <https://www.bleepingcomputer.com/news/security/mirai-botnet-variants-targeting-new-processors-and-architectures/>.
- 36 Sean Gallagher, *New variants of Mirai botnet detected, targeting more IoT devices*, Ars Technica (Apr. 9, 2019, 1:49 PM), <https://arstechnica.com/information-technology/2019/04/new-variants-of-mirai-botnet-detected-targeting-more-iot-devices/>.
- 37 Charles DeBeck, Joshua Chung & Dave McMillen, *I Can't Believe Mirais: Tracking the Infamous IoT Malware*, SecurityIntelligence (July 18, 2019), <https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/>.
- 38 Derek Manky, *The Evolving Threat Landscape – Swarbots, Hivenets, Automation in Malware*, CSO (Aug. 29, 2018, 9:00 AM), <https://www.csoonline.com/article/3301148/the-evolving-threat-landscape-swarbots-hivenets-automation-in-malware.html>.
- 39 Derek Manky, *Rise of the 'Hivenet': Botnets That Think for Themselves*, DarkReading (Feb. 16, 2018, 10:30 AM), <https://www.darkreading.com/vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/a/d-id/1331062>.
- 40 Derek Manky, *Rise of the 'Hivenet': Botnets That Think for Themselves*, DarkReading (Feb. 16, 2018, 10:30 AM), <https://www.darkreading.com/vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/a/d-id/1331062>.
- 41 Derek Manky, *The Evolving Threat Landscape – Swarbots, Hivenets, Automation in Malware*, CSO (Aug. 29, 2018, 9:00 AM), <https://www.csoonline.com/article/3301148/the-evolving-threat-landscape-swarbots-hivenets-automation-in-malware.html>.
- 42 Derek Manky, *The Evolving Threat Landscape – Swarbots, Hivenets, Automation in Malware*, CSO (Aug. 29, 2018, 9:00 AM), <https://www.csoonline.com/article/3301148/the-evolving-threat-landscape-swarbots-hivenets-automation-in-malware.html>.
- 43 Colin Grady, William Largent & Jaeson Schultz, *Emotet is back after a summer break*, Cisco Talos Intelligence Group (Sept. 17, 2019), <https://blogs.cisco.com/security/talos/emotet-is-back-after-a-summer-break>.
- 44 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (Sept. 19, 2019, 2:45 PM), <https://arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/>.
- 45 *Analyzing the botnet infrastructure and threat actors behind TrickBot*, NTT (Mar. 28, 2019), <https://technical.nttsecurity.com/post/102fhgo/analyzing-the-botnet-infrastructure-and-threat-actors-behind-trickbot>.
- 46 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (Sept. 19, 2019, 2:45 PM), <https://arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/>.
- 47 Colin Grady, William Largent & Jaeson Schultz, *Emotet is back after a summer break*, Cisco Talos Intelligence Group (Sept. 17, 2019), <https://blog.talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html>.

- 48 Colin Grady, William Largent & Jaeson Schultz, *Emotet is back after a summer break*, Cisco Talos Intelligence Group (Sept. 17, 2019), <https://blog.talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html>.
- 49 Dan Goodin, *World's most destructive botnet returns with stolen passwords and email in tow*, Ars Technica (Sept. 19, 2019, 2:45 PM), <https://arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/>.
- 50 Catalin Cimpanu, *Emotet, today's most dangerous botnet, comes back to life*, ZDNet (Sept. 16, 2019), <https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/>.
- 51 Catalin Cimpanu, *Necurs and Gamut Botnets Account for 97% of the Internet's Spam Emails*, BleepingComputer (Mar. 12, 2018, 5:20 AM), <https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/>.
- 52 *Email: Click with Caution*, Cisco 31, <https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf> (last visited Oct. 8, 2019).
- 53 *2019 Threat Report*, CenturyLink 19, <https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf> (last visited Oct. 8, 2019).
- 54 Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CyberScoop (Oct. 27, 2016), <https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web>.
- 55 Derek Manky, *The Evolving Threat Landscape – Swarmbots, Hivenets, Automation in Malware*, CSO (Aug. 29, 2018, 9:00 AM), <https://www.csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html>.
- 56 Catalin Cimpanu, *Liberian ISP sues rival for hiring hacker to attack its network*, ZDNet (Jan. 14, 2019), <https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network>.
- 57 Catalin Cimpanu, *Liberian ISP sues rival for hiring hacker to attack its network*, ZDNet (Jan. 14, 2019), <https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network>.
- 58 Catalin Cimpanu, *Liberian ISP sues rival for hiring hacker to attack its network*, ZDNet (Jan. 14, 2019), <https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network>.
- 59 Curtis Franklin Jr., *New Botnet Shows Evolution of Tech and Criminal Culture*, DarkReading (Feb. 4, 2019, 6:30 PM), <https://www.darkreading.com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal-culture/d/d-id/1333792>.
- 60 Curtis Franklin Jr., *New Botnet Shows Evolution of Tech and Criminal Culture*, DarkReading (Feb. 4, 2019, 6:30 PM), <https://www.darkreading.com/attacks-breaches/new-botnet-shows-evolution-of-tech-and-criminal-culture/d/d-id/1333792>.
- 61 Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 5, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf> (last visited Oct. 8, 2019).
- 62 Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 5, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf> (last visited Oct. 8, 2019).
- 63 Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 18, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf> (last visited Oct. 8, 2019).
- 64 Jay Coley, *Bots try to break the internet, and other trends for 2019*, TechRadar (Feb. 21, 2019), <https://www.techradar.com/news/bots-try-to-break-the-internet-and-other-trends-for-2019>.
- 65 Akamai, *DDoS and Application Attacks*, State of the Internet Security 17, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf> (last visited Oct. 8, 2019).
- 66 *The Rise of "Bulletproof" Residential Networks*, KrebsOnSecurity (Aug. 19, 2019), <https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks>.
- 67 Akamai, *DDoS and Application Attacks*, State of the Internet Security 18, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf> (last visited Oct. 8, 2019).
- 68 Charlie Osborne, *New Mirai botnet lurks in the Tor network to stay under the radar*, ZDNet (Aug. 1, 2019), <https://www.zdnet.com/article/new-mirai-botnet-lurks-in-the-tor-network-to-stay-under-the-radar>.
- 69 Tara Seals, *Necurs Botnet Evolves to Hide in the Shadows, with New Payloads*, Threatpost (Mar. 1, 2019, 10:41 AM), <https://threatpost.com/necurs-botnet-hide-payloads/142334>.
- 70 *Casting Light On The Necurs Shadow*, CenturyLink (Feb. 28, 2019), <https://blog.centurylink.com/casting-light-on-the-necurs-shadow>.
- 71 *Casting Light On The Necurs Shadow*, CenturyLink (Feb. 28, 2019), <https://blog.centurylink.com/casting-light-on-the-necurs-shadow>.
- 72 *See Akamai, Retail Attacks and API Traffic*, State of the Internet Security 5, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf> (last visited Oct. 8, 2019).
- 73 *The Rise of "Bulletproof" Residential Networks*, Krebs on Security (Aug. 19, 2019), <https://krebsonsecurity.com/2019/08/the-rise-of-bulletproof-residential-networks>.
- 74 Robin Kurzer, *Oracle discovers another major fraud operation affecting Android users and mobile advertisers*, Marketing Land (Feb. 20, 2019, 7:00 AM), <https://marketingland.com/oracle-discovers-another-major-fraud-operation-affecting-android-users-and-mobile-advertisers-257322>.
- 75 Conor Reynolds, *Botnet Attacks: From DDoS to Hivenets and Sextortion*, CBR (Aug. 29, 2019), <https://www.cbronline.com/feature/botnet-attacks-changing-theatre>.
- 76 Robin Kurzer, *Oracle discovers another major fraud operation affecting Android users and mobile advertisers*, Marketing Land (Feb. 20, 2019, 7:00 AM), <https://marketingland.com/oracle-discovers-another-major-fraud-operation-affecting-android-users-and-mobile-advertisers-257322>.
- 77 Jeff Stone, *From DDoS attacks to ad fraud: Smarter bots are copying human behavior*, CyberScoop (Dec. 10, 2018), <https://www.cyberscoop.com/smart-botnet-human-behavior-ddos-ad-fraud-methbot>.
- 78 Jeff Stone, *From DDoS attacks to ad fraud: Smarter bots are copying human behavior*, CyberScoop (Dec. 10, 2018), <https://www.cyberscoop.com/smart-botnet-human-behavior-ddos-ad-fraud-methbot>.
- 79 *See Telefonica, Etisalat & Singtel, Twitter botnets detection in sports events*, Trend Report, <https://www.elevenpaths.com/wp-content/uploads/2018/12/twitter-botnets-detection-in-sports-events.pdf> (last visited Oct. 8, 2019).
- 80 Christine Fisher, *Twitter bans thousands of state-backed accounts spreading misinformation*, Engadget (Sept. 20, 2019), <https://www.engadget.com/2019/09/20/twitter-bans-state-backed-misinformation>.



- 81 Ben Collins & Shoshana Wodinsky, *Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist*, NBCNews (Oct. 18, 2018, 6:39 PM), <https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871>.
- 82 Jessica Lyons Hardcastle, *Cyber Threat Alliance Reports 459% Spike in Cryptomining Malware*, SDxCentral (Sept. 21, 2018, 1:18 PM), <https://www.sdxcentral.com/articles/news/cyber-threat-alliance-459-spike-cryptomining-malware/2018/09>.
- 83 Catalin Cimpanu, *Crypto-mining malware saw new life over the summer as Monero value tripled*, ZDNet (Sept. 18, 2019), <https://www.zdnet.com/article/crypto-mining-malware-saw-new-life-over-the-summer-as-monero-value-tripled>.
- 84 Michael Nadeau, *What is cryptojacking? How to prevent, detect, and recover from it*, CSO (Aug. 2, 2019, 3:00 AM), <https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>.
- 85 *The Illicit Cryptocurrency Mining Threat*, Cyber Threat Alliance 4, <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf> (last visited Oct. 8, 2019).
- 86 *The Illicit Cryptocurrency Mining Threat*, Cyber Threat Alliance 15, <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf> (last visited Oct. 8, 2019).
- 87 Catalin Cimpanu, *Two crypto-mining groups are fighting a turf war over unsecured Linux servers*, ZDNet (May 10, 2019), <https://www.zdnet.com/article/two-crypto-mining-groups-are-fighting-a-turf-war-over-unsecured-linux-servers/>.
- 88 Lucian Constantin, *Secrets of latest Smominru botnet warrant revealed in new attack*, CSO (Sept. 18, 2019, 6:00 AM), <https://www.csoonline.com/article/3439400/secrets-of-latest-smominru-botnet-variant-revealed-in-new-attack.html>.
- 89 Catalin Cimpanu, *Two botnets are fighting over control of thousands of unsecured Android devices*, ZDNet (Nov. 2, 2018), <https://www.zdnet.com/article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured-android-devices>.
- 90 Tara Seals, *MyloBot Botnet Emerges with Rare Level of Complexity*, Threatpost (June 20, 2018, 1:12 PM), <https://threatpost.com/mylobot-botnet-emerges-with-rare-level-of-complexity/132967>.
- 91 Catalin Cimpanu, *A mysterious grey-hat is patching people's outdated MikroTik routers*, ZDNet (Oct. 12, 2018), <https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers>.
- 92 Mark Samuels, *Vigilante White-Hat Hacker Boosts IoT Device Security*, SecurityIntelligence (Apr. 20, 2017, 1:31 PM), <https://securityintelligence.com/news/vigilante-white-hat-hacker-boosts-iot-device-security>.
- 93 RFC 2460 Network Working Group, *Internet Protocol, Version 6 (IPv6) Specification*, IETF (Dec. 1998), <https://tools.ietf.org/html/rfc2460>.
- 94 Marek Šimon & Ladislav Huraj, *A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks*, SpringerLink, [https://link.springer.com/chapter/10.1007/978-3-030-19807-7\\_12](https://link.springer.com/chapter/10.1007/978-3-030-19807-7_12) (last visited Oct. 10, 2019).
- 95 Erik Nygren, *Six Years Since World IPv6 Launch: Entering the Majority Phases*, Akamai (June 6, 2018, 12:00 PM), <https://blogs.akamai.com/2018/06/six-years-since-world-ipv6-launch-entering-the-majority-phases.html>.
- 96 Akamai, *Retail Attacks and API Traffic*, State of the Internet Security 4, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf> (last visited Oct. 10, 2019).
- 97 Kelly Hill, *Netscout: IoT devices under attack within minute of turn-up*, RCRWirelessNews (Aug. 6, 2019), <https://www.rcrwireless.com/20190806/internet-of-things/netscout-iot-devices-under-attack-within-minutes-of-turn-up>.
- 98 Martin Zeiser & Aleksandar Nikolich, *IPv6 unmaking via UPnP*, Cisco (Mar. 18, 2019), <https://blog.talosintelligence.com/2019/03/ipv6-unmasking-via-upnp.html>.
- 99 Rene Paap, *IPv6 And the Growing DDoS Danger*, DarkReading (Nov. 2, 2015, 10:30 AM), <https://www.darkreading.com/attacks-breaches/ipv6-and-the-growing-ddos-danger/a/d-id/1322942>.
- 100 Kieren McCarthy, *It's begun: 'First' IPv6 denial-of-service attacks puts IT bods on notice*, The Register (Mar. 3, 2018, 9:30 AM), [https://www.theregister.co.uk/2018/03/03/ipv6\\_ddos/](https://www.theregister.co.uk/2018/03/03/ipv6_ddos/).
- 101 Mark Mayne, *'First true' native IPv6 DDoS attack spotted in wild*, SCMedia (Feb. 28, 2018), <https://www.scmagazineuk.com/first-true-native-ipv6-ddos-attack-spotted-wild/article/1473177>.
- 102 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, NIST (May 22, 2018), available at <https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft>; Comm'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), available at [https://transition.fcc.gov/pshs/advisory/csrc4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csrc4/CSRIC_IV_WG4_Final_Report_031815.pdf); ENISA, Botnet Measurement, Detection, Disinfection and Defence (Mar. 7, 2011), <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>; Int'l Telecomm. Union, ITU Botnet Mitigation Toolkit (Jan. 2008), <https://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>.
- 103 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (May 22, 2018), available at <https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft>.
- 104 Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 7–9 (Sept. 2017) (discussing tools and techniques for DDoS protection, including ingress/egress filtering; on-premise and off-premise DDoS protection), available at <https://doi.org/10.6028/NIST.IR.8192>; see also, Ctr. for Democracy and Tech, Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats 2 (Feb. 12, 2018) (agreeing with the NTIA's draft report that "common techniques for botnet mitigation include ingress and egress filtering, re-routing and shaping internet traffic, and isolating devices or other entities."), available at <https://cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf>; Comm'n Sec., Reliability and Interoperability Council IV Working Group 4, *Final Report on Cybersecurity Risk Management and Best Practices* (Mar. 2015), available at [https://transition.fcc.gov/pshs/advisory/csrc4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csrc4/CSRIC_IV_WG4_Final_Report_031815.pdf).
- 105 See, e.g., United States, DHS Automated Indicator Sharing (AIS) System, <https://www.us-cert.gov/ais> (last accessed Oct. 17, 2018); United Kingdom, Cyber Security Information Sharing Partnership (CISIP), <https://www.ncsc.gov.uk/section/keep-up-to-date/cisip> (last accessed Oct. 17, 2018); Japan, Cyber Clean Center, [https://www.telecom-isac.jp/ccc/en\\_index.html](https://www.telecom-isac.jp/ccc/en_index.html) (last accessed Oct. 17, 2018); New Zealand, CORTEX, <https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs> (last accessed Oct. 17, 2018).

- 106 See David Strom, *What Is Polymorphic Malware and Why Should I Care?* (Oct. 16, 2015), <https://securityintelligence.com/what-is-polymorphic-malware-and-why-should-i-care>.
- 107 Verizon, 2012 *Data Breach Investigations Report 71* (2012), [https://www.wired.com/images\\_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf](https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf).
- 108 See Stephen Sladartitz, *About Heuristics*, SANS Institute 4 (Mar. 23, 2002), available at <https://www.sans.org/reading-room/whitepapers/malicious/about-heuristics-141> (comparing the two different types of heuristic analysis); see also John Aycok, *Computer Viruses and Malware 74* (2006) (explaining that the only difference between static and dynamic heuristics is “how the data is gathered” and otherwise the data is identical).
- 109 See, e.g., Cisco, *Cisco Cognitive Threat Analytics v1* (Feb. 2016), [https://dcloud.cms.cisco.com/demo\\_news/cisco-cognitive-threat-analytics-v1](https://dcloud.cms.cisco.com/demo_news/cisco-cognitive-threat-analytics-v1).
- 110 Nat’l Inst. of Standards and Tech., *Advanced DDoS Mitigation Techniques* (Oct. 18, 2017) (“For well over a decade industry had developed specifications of techniques and deployment guidance for IP-level filtering techniques to block network traffic with spoofed source addresses”), available at <https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques>.
- 111 Ferguson & D. Senie, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, Internet Engineering Task Force (IETF) Network Working Group (May 2000), available at <https://tools.ietf.org/html/bcp38>; F. Baker & P. Savola, *Ingress Filtering for Multihomed Networks*, Internet Engineering Task Force (IETF) Network Working Group (Mar. 2004), available at <https://tools.ietf.org/html/bcp84>.
- 112 *Id.*
- 113 See generally, e.g., Chris Benton, *Egress Filtering FAQ*, SANS Institute (Apr. 19, 2006), available at <https://www.sans.org/reading-room/whitepapers/firewalls/egress-filtering-faq-1059>.
- 114 See Cisco, *Access Control Lists* (last updated July 17, 2018), <https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asdm79/firewall/asdm-79-firewall-config/access-acls.html>.
- 115 See Cisco, *Policing and Shaping Overview* (last updated Nov. 23, 2017), [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-overview.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-overview.html).
- 116 See generally, e.g., Guy Bruneau, *DNS Sinkhole*, SANS Institute (Aug. 7, 2010), <https://isc.sans.edu/forums/diary/DNS+Sinkhole+ISO+Version+20/21153/>.
- 117 See Cisco, *Implementing BGP Flowspec* (last updated Jan. 31, 2018), [https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k\\_r5-2/routing/configuration/guide/b\\_routing\\_cg52xasr9k/b\\_routing\\_cg52xasr9k\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.html).
- 118 See Georgia Tech Researchers, *DNS Changer Remediation Study, Presentation to M3AAWG 27th General Meeting, San Francisco, CA* (Feb. 19, 2013), available at <https://www.m3aawg.org/news/independent-georgia-tech-study-reveals-best-ways-to-tell-customers-“you’re-botted”> (last accessed Oct. 17, 2018); see also Comm’n Sector Coordinating Council, Botnet Whitepaper 24–25 (July 17, 2017) (listing multiple ways that infrastructure providers can notify users, including email, telephone call, postal mail, text message, web browser notification, walled garden, and other methods such as social media), available at [https://docs.wixstatic.com/ugd/0a1552\\_18ae07afc1b04aa1bd13258087a9c77b.pdf](https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf).
- 119 See Ctr. for Democracy and Tech, Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares (Nov. 14, 2011) (expressing concern about the practice of “cutting off or otherwise interfering with a customer’s Internet connection” to compel botnet remediation), available at <https://www.nist.gov/sites/default/files/documents/itl/CDT-Comments-on-BotNet-FRN-11-14-11.pdf>; Elec. Frontier Found., Comments to the NIST Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malwares 5 (Nov. 14, 2011) (explaining how uninfected parties could have their internet access affected by quarantine), available at <https://www.nist.gov/sites/default/files/documents/itl/AT-Ts-Comments-to-BotNet-FRN-11-14-11.pdf>.
- 120 See Comm’n Sector Coordinating Council, Botnet Whitepaper 21 (July 17, 2017), (“No technique is more effective than law enforcement actions that lead to the arrest of the perpetrators. This is the only solution that addresses the root cause of the problem, and not just a symptom... [E]xecuting a botnet takedown requires significant upfront forensic analysis and careful coordination among many stakeholders, often across international borders.... Most botnets are international in nature, requiring resource-intensive and time-consuming cooperation between nations.”), available at [https://docs.wixstatic.com/ugd/0a1552\\_18ae07afc1b04aa1bd13258087a9c77b.pdf](https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf).
- 121 See Robert Wainright and Frank J. Cilluffo, Responding to Cyber Crime at Scale: A Case Study, Europol & the George Washington Univ. Ctr. for Cyber and Homeland Sec. (Mar. 2017), available at <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf>.
- 122 See SAFECode, *Fundamental Practices for Secure Software Development* (Mar. 2018), [https://safecode.org/wp-content/uploads/2018/03/SAFECode\\_Fundamental\\_Practices\\_for\\_Secure\\_Software\\_Development\\_March\\_2018.pdf](https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf).
- 123 Arora et al., *An Empirical Analysis of Software Vendors’ Patching Behavior: Impact of Vulnerability Disclosure*, Carnegie Mellon University (Jan. 2006) (analyzing incentives of larger vendors relative to other vendors), available at [https://www.heinz.cmu.edu/~rtelang/disclosure\\_jan\\_06.pdf](https://www.heinz.cmu.edu/~rtelang/disclosure_jan_06.pdf).
- 124 See SAFECode, *Principles for Software Assurance Assessment* (2015), available at [https://safecode.org/wp-content/uploads/2015/11/SAFECode\\_Principles\\_for\\_Software\\_Assurance\\_Assessment.pdf](https://safecode.org/wp-content/uploads/2015/11/SAFECode_Principles_for_Software_Assurance_Assessment.pdf).
- 125 Nat’l Inst. of Standards and Tech., *NTIA Software Component Transparency* (Oct. 21, 2019), <https://www.ntia.doc.gov/SoftwareTransparency>.
- 126 Council to Secure the Digital Economy, *The C2 Consensus on IoT Device Security Baseline Capabilities* (2019), [https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE\\_IoT-C2-Consensus-Report\\_FINAL.pdf](https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf).
- 127 Early requirements planning and ultimately certification is essential to this process. For example, CTIA manages a certification program for IoT devices, establishing industry requirements for device security on wireless networks and providing a certification program. Details on the program, including requirements and how to certify a device, can be found here: <https://www.ctia.org/about-ctia/programs/certification-resources>.
- 128 See Microsoft, *What is the Security Development Lifecycle?*, <https://www.microsoft.com/en-us/sdl/default.aspx> (last accessed Oct. 19, 2018).
- 129 See BSIMM, <https://bsimm.com> (last accessed Nov. 6, 2018).
- 130 For more international standards, see Nat’l Inst. of Standards and Tech., *Cryptographic Module Validation Program*, <https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards>. In addition, NIST has a draft summary of international standards: Nat’l Inst. of Standards and Tech., *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, <https://csrc.nist.gov/publications/detail/nistir/8200/draft> (last accessed Oct. 10, 2018).
- 131 *Id.*



- 132 For a discussion on updates, see Nat'l Inst. Of Standards and Tech., *Stakeholder-Drafted Documents on IoT Security*, <https://www.ntia.doc.gov/IoTSecurity> (last accessed Oct. 10, 2018).
- 133 *Manufacturer Usage Description Specification*, IETF (Mar. 19, 2019), <https://datatracker.ietf.org/doc/rfc8520/>.
- 134 See *OMA Device Management Overview* (Apr. 20, 2018), [http://www.openmobilealliance.org/wp/overviews/dm\\_overview.html](http://www.openmobilealliance.org/wp/overviews/dm_overview.html).
- 135 See *CPE WAN Management Protocol*, Broadband Forum (Mar. 2018), <https://www.broadband-forum.org/download/TR-069.pdf>.
- 136 Bruhadeshwar Bezawada et al., *IoT Sense: Behavioral Fingerprinting of IoT Devices*, Colorado State University (Apr. 2018), <https://arxiv.org/pdf/1804.03852.pdf>.
- 137 Consumer Technology Association, *The Connected Home Security System*, <https://cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx> (last visited Oct. 10, 2018).
- 138 U.S. Dep't of Commerce & U.S. Dep't of Homeland Sec., *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* 12–15 (May 22, 2018), available at [https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo\\_13800\\_botnet\\_report\\_-\\_finalv2.pdf](https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf).
- 139 Cybersecurity Coalition, *DDoS Threat Mitigation Profile*, <https://www.cybersecuritycoalition.org/ddos-framework> (last accessed Nov. 14, 2018), and Cybersecurity Coalition, *Botnet Threat Mitigation Profile*, <https://www.cybersecuritycoalition.org/botnet-framework> (last accessed Nov. 14, 2018).
- 140 See Comm'n Sec., Reliability and Interoperability Council II Working Group 8, *Final Report on ISP Network Protection 16* (recommending, *inter alia*, that users should "[c]onfigure [the] computer to download critical updates to both the operating system and installed applications automatically.") (Nov. 2011), available at [https://transition.fcc.gov/pshs/docs/csric/CSRIC\\_WG8\\_FINAL\\_REPORT\\_ISP\\_NETWORK\\_PROTECTION\\_20101213.pdf](https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf).
- 141 Tim Polk, *Enhancing Resilience of the Internet and Communications Ecosystem*, Nat'l Inst. of Standards and Tech. 13 (Sept. 2017) (citing opinions of participants in the NIST Enhancing Resilience of the Internet and Communications Ecosystem workshop on July 11-12, 2017), available at <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8192.pdf>.
- 142 Scott Bowen, Akamai, *Defense By Design: How To Dampen DDoS Attacks With A Resilient Network*, Forbes (Sept. 14, 2017) <https://www.forbes.com/sites/akamai/2017/09/14/defense-by-design-how-to-dampen-ddos-attacks-with-a-resilient-network/#79144da56f8a>.
- 143 See, e.g., AT&T, *Distributed Denial of Service (DDoS) Defense* (2014), available at [https://www.business.att.com/content/productbrochures/ddos\\_prodbrief.pdf](https://www.business.att.com/content/productbrochures/ddos_prodbrief.pdf); Verizon, *DDoS Shield Solutions Brief* (2016), available at [http://www.verizonenterprise.com/resources/ddos\\_shield\\_solutions\\_brief\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/ddos_shield_solutions_brief_en_xg.pdf); CenturyLink, *DDoS Mitigation* (2014), available at <http://www.centurylink.com/asset/business/enterprise/brochure/ddos-mitigation.pdf>; Telefonica, *Anti-DDoS*, <https://www.elevenpaths.com/technology/anti-ddos/index.html> (last visited Nov. 3, 2019); NTT, *DDoS Protection Service*, <https://www.ntt.com/en/services/network/gin/transit/ddos.html> (last visited May 14, 2018).
- 144 See discussion *supra* Part 5.A.2(e) (explaining the function of scrubbing centers in mitigating botnets).
- 145 Nat'l Inst. of Standards and Tech., *Digital Identity Guidelines* (June 2017), available at <https://doi.org/10.6028/NIST.SP.800-63-3>.
- 146 Brian Krebs, *Google: Security Keys Neutralized Employee Phishing*, Krebs on Security (July 23, 2018) <https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing>.
- 147 See Microsoft, *Windows XP Support has ended*, <https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support> (last visited May 15, 2018).
- 148 See BSA The Software Alliance, *Seizing Opportunity Through License Compliance: BSA Global Software Survey 6–7* (2016), <https://globalstudy.bsa.org/2016/>.
- 149 *Id.* at 4 (discussing the “strong correlation” between malware and unlicensed software).
- 150 National University of Singapore, *Cybersecurity Risks from Non-Genuine Software, The Link Between Pirated Software Sources and Cybercrime Attacks in Asia Pacific* 6 (Nov. 1, 2017), <https://news.microsoft.com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf> (“[I]n many parts of the world, the use of pirated/counterfeit/non-genuine software is a serious contributor to the growth of cyber-risks and is responsible for extensive economic harm and productivity losses. It is also causing a rise in cybercrime attacks and related losses.”)

For additional information on the  
Council to Secure the Digital Economy  
([securingdigitaleconomy.org](http://securingdigitaleconomy.org))  
or information on this report,  
please contact:

**Robert Mayer**

Senior Vice President - Cybersecurity  
USTelecom  
[rmayer@ustelecom.org](mailto:rmayer@ustelecom.org)

**Mike Bergman**

Vice President - Technology & Standards  
Consumer Technology Association  
[mbergman@cta.tech](mailto:mbergman@cta.tech)



[securingsdigitaleconomy.org](https://securingsdigitaleconomy.org)

# Cyber Crisis: Foundations of Multi-Stakeholder Coordination



Council to Secure the  
Digital Economy

USTELECOM  
THE BROADBAND ASSOCIATION

Consumer Technology  
Association™

**In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. This guide draws on the diverse international perspectives of CSDE members, as well as their leading practices and real-world actions, to increase incident response readiness, capabilities, and cooperation during catastrophic, crisis-level incidents that call for mobilization of the Information and Communications Technology (ICT) sector.**





# Cyber Crisis: Foundations of Multi-Stakeholder Coordination





## Contents

<b>01</b>	Executive Summary .....	1
<b>02</b>	Introduction.....	5
<b>03</b>	Overview of Global ICT Segments Represented in the CSDE.....	8
<b>04</b>	Private Sector Cyber Crisis Assets and Capabilities .....	11
<b>05</b>	Public-Private Coordination in Cyber Crisis Scenarios.....	16
<b>06</b>	International Coordination.....	25
<b>07</b>	Next Steps.....	27
<b>08</b>	Appendix A: Cyber Crisis Scenarios Examined by the CSDE.....	28
<b>09</b>	Endnotes .....	41

## 01 | Executive Summary

**THE MEMBERS OF** the Council to Secure the Digital Economy (CSDE) cover the complex global internet and communications ecosystem. In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. In recent years, we have seen cyber-attacks against power plants, oil and gas companies, financial centers, military organizations, hospitals, governments, and virtually every other institution that supports modern civilization.<sup>1</sup> In the midst of a cybersecurity crisis, government and industry must be prepared to mobilize rapidly and collaborate with relevant responders. This response should be framed in the context of voluntary frameworks where industry leads decisively by leveraging the mature assets and capabilities of Information and Communications Technology (ICT) companies.

Different types of ICT companies, many of which are represented in the CSDE's membership, are likely to be essential during one or more categories of potentially catastrophic cyber events. In order for governments to determine the most relevant, leverageable assets and capabilities of any given company, they should build close working relationships with the companies whose leadership and experience in responding to high-level cyber incidents makes them valuable partners in the global fight against cyber threats. Increasingly, policymakers have recognized the need for international cooperation and coordination to address the growing epidemic of cyber-attacks.

**Deploying Security Teams in a Cyber Crisis.** As primary drivers of technological innovation and progress across the globe, leading ICT companies have at their collective disposal some of the world's most advanced cybersecurity and incident response assets; these range from state-of-the-art operations facilities with sophisticated mitigation tools, technologies, and processes to experienced teams of cybersecurity experts who are qualified to handle crisis-level events.

The following is not intended to be a comprehensive listing of ICT assets and capabilities, but rather an executive overview of high-value resources and considerations for mitigating cybersecurity incidents.

- ▶ **Threat Intelligence Sharing Partnerships** — Omni-directional partnerships across the cybersecurity community facilitate the exchange of vital threat intelligence with both public and private sector partners, and with governmental agencies around the globe.
- ▶ **IP Network Operations Center (IP NOC)** — A facility designed to enable management of an IP network to preserve infrastructure integrity and functionality. The IP NOC will typically be staffed by human operators, such as security engineers, who are well-trained at interpreting the data traveling through the network.
- ▶ **Security Operations Center (SOC)** — The central team within an organization responsible for cybersecurity. It oversees the human and technological processes and operations necessary to defend against cyber threats.
- ▶ **Computer Security Incident Response Team (CSIRT)** — This team is activated only during critical cyber-attacks or vulnerabilities and often employs a structure that is compatible with well recognized best practices that enable a company to swiftly take action during crisis events.
- ▶ **Product Security Incident Response Team (PSIRT)** — An entity within an organization that focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within the products.<sup>2</sup>

- ▶ **Cybersecurity Vulnerability Assessors** — Experts who are trained to discover actual or possible exposure to cyber threats and conduct in-depth analysis of an organization's security posture.
- ▶ **Security Engineers and Other Cybersecurity Professionals** — Security engineers are cybersecurity professionals whose job is to protect and mitigate against cyber threats.
- ▶ **Subject Matter Experts** — In responding to cyber incidents, companies may leverage input from experts (either in-house or external to the organization) that are recognized for their specialized knowledge in relevant fields of cybersecurity.

**Identifying Potential Responders During Cyber Crises.** Based on an extensive survey of CSDE members, we developed an understating of the likely roles of different ICT segments in each of the scenarios analyzed. This understanding is represented below and, although subject to changes based on the situational realities “on the ground” during an incident, should serve as effective general guidance for private and public ICT stakeholders.

We recognize that distinct frameworks can provide guidance in different scenarios. Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. Combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.

In addition, major companies represented in the CSDE, even if not directly relevant to a resolving a security issue, may be able to help government or industry partners quickly identify relevant ICT companies (infrastructure, software, hardware, security service providers, and others) in the initial triage stage of a potential or actual crisis, in order to facilitate and expedite critical response efforts. Further, these same companies may be in the best position to provide meaningful support in implementing the joint response.

### DDoS Attacks

- ▶ **Scenarios Examined:** DDoS Botnet Attack; DDoS Server-based Attack
- ▶ **Potential Responders:** Situationally relevant Infrastructure Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers

### Internet Traffic Hijacking

- ▶ **Scenarios Examined:** Border Gateway Protocol (BGP) Hijacking; Domain Name System (DNS) Hijacking
- ▶ **Potential Responders for BGP Hijacking:** Situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors; Managed Security Service Providers
- ▶ **Potential Responders for DNS Hijacking:** DNS Providers; situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors



### Software Vulnerabilities

- ▶ **Scenarios Examined:** Open Source Vulnerabilities; Zero Day Vulnerabilities
- ▶ **Potential Responders:** Situationally relevant Software Vendors; Original Software Developers (OSDs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

### Hardware Vulnerabilities

- ▶ **Scenarios Examined:** Processor or Component Vulnerabilities
- ▶ **Potential Responders:** Situationally relevant Hardware Vendors; Original Equipment Manufacturers (OEMs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

### Software and Hardware Component Backdoors

- ▶ **Scenarios Examined:** Injection of Malicious Code in Software and Hardware Components
- ▶ **Potential Responders:** Same potential responders as Software and Hardware Vulnerabilities respectively

### Malware and Ransomware

- ▶ **Scenarios Examined:** Destructive Malware; Ransomware
- ▶ **Potential Responders:** Situationally relevant Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

### Advanced Persistent Threats (APTs) and Cloud Compromises

- ▶ **Scenarios Examined:** Advanced Persistent Threat (APT); Industrial Systems; Cloud Provider Compromise
- ▶ **Potential Responders:** Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

**Strengthening Relationships and Cooperation.** The CSDE considered the global stakeholder community when developing this voluntary guide. In order to harmonize operations in the event of cybersecurity crises that call for private sector mitigations efforts, we will share this guide with a broad set of stakeholders throughout the ecosystem and undertake concerted efforts to encourage participation by key trusted companies in incident response efforts for the security of our digital economy. We will also build awareness of the diverse national and global venues where cyber incident response can be operationalized.

By strengthening the relationships among key stakeholders, as well as developing guides to mitigate specific kinds of cyber threats and vulnerabilities, the CSDE will continue to serve as a critical forum for cyber policy leaders representing global ICT companies that are on the front lines during cyber-attacks and are committed to securing the digital economy.

## 02 | Introduction

**THE MEMBERS OF** the Council to Secure the Digital Economy (CSDE) cover the complex global internet and communications ecosystem — including the many human and technical systems that create, deploy, and manage the infrastructure, software, and devices that benefit a significant portion of the world's consumers, small businesses, large private enterprises, governments, and non-profits — collectively, the global digital economy.

In this guide, we lay the foundations for multi-stakeholder coordination during cybersecurity crises that can undermine the security of the digital economy. This guide draws on the diverse international perspectives of CSDE members, as well as their leading practices and real-world actions, to increase incident response readiness, capabilities, and cooperation during catastrophic, crisis-level incidents that call for mobilization of the Information and Communications Technology (ICT) sector.

We recognize that distinct frameworks can provide guidance in different scenarios. Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. Combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.

**Global Cyber Crises: More Frequent, More Costly, and More Dangerous.** The digital economy is producing immense benefits for the world that must be defended against aggressive actions and potentially devastating cyber events. By some estimates, the digital economy may already represent 20% of global economic value,<sup>3</sup> and although GDP alone cannot capture the full worth of the digital economy, the projected value of the digital economy by 2025 is \$23 trillion — almost a quarter of global GDP.<sup>4</sup> The digital economy has generated quality-of-life improvements on every continent, created whole new industries and millions of jobs, and increased efficiency in every sector.

At the same time, the asymmetry between the relatively low cost of launching highly disruptive cyber-attacks and the high cost to defend against such attacks, among other factors, has created harmful incentives for sophisticated actors, including nation states that wish to project power and influence in global affairs. In recent years, we have seen criminal and politically motivated attacks on critical infrastructure, as well as other illicit operations such as cyber espionage and ransomware of critical data. These emerging trends could result in massive economic damage and undermine confidence in the digital economy, which is an outcome the CSDE was created to prevent.

The economic and public safety consequences of cyber-attacks have increased severely in recent years. An attack against a cloud service provider could cause tens of billions of dollars in damage, and one study estimates that a single cloud event can cost up to \$120 billion, a figure that exceeds some of the worst natural disasters.<sup>5</sup> We have seen cyber-attacks against power plants, oil and gas companies, financial centers, military organizations, hospitals, governments, and virtually every other institution that supports modern civilization.<sup>6</sup>

It is clear that cyber-attacks have reached the level of a sustained crisis in some parts of the world. For example, in 2015, a cyber-attack caused people in Ukraine to lose electricity for six hours in the middle of winter.<sup>7</sup> In 2017, an attack against the same country's financial systems escalated into an international epidemic that caused over \$10 billion damage worldwide.<sup>8</sup> This was the costliest cyber-attack in history,<sup>9</sup> but much more damaging attacks are possible.

Researchers continue to discover malware targeted against specific geopolitical targets in many parts of the world.<sup>10</sup> In a shared internet and communications ecosystem, attacks targeted at specific nations can and often do have spillover effects that are damaging for broad sets of stakeholders — not just the intended targets.<sup>11</sup> Hence, whether dealing with hacking groups sponsored by nation states with geopolitical ambitions or sophisticated cybercriminal organizations with profit-driven goals, like-minded governments and industry alliances have enormous incentives to curtail the most damaging actions in cyberspace and unite against common threats to the shared digital ecosystem.

It is not merely a matter of ethical necessity and building mutually beneficial relationships; it is also a matter of protecting each nation's economic and security interests.

**Industry Provides Leadership in a Cyber Crisis.** The CSDE recognizes the need for industry leadership and collaboration with government partners during major cyber incidents. As the capabilities of well-financed and sophisticated malicious actors reach new levels of maturity, dangers in the cyber threat environment increasingly pose global and ecosystem-wide economic security challenges that exceed the individual response capabilities of any single company or industrial sector.

The widespread and consequential nature of the most serious cyber threats requires ICT companies — particularly companies with assets and capabilities that may be necessary to support incident response during cyber incidents — to recognize shared dependencies and responsibilities as stewards of the digital economy and jointly coordinate actions necessary for immediate response to and recovery from catastrophic scenarios. The CSDE's diverse and global members, which include ICT companies across the internet and communications ecosystem, are excellently positioned to provide the guidance, insight, and leadership needed for their respective ecosystem segments.

In the midst of a cybersecurity crisis, government and industry must be prepared to mobilize rapidly and collaborate with relevant responders. This response should be framed in the context of voluntary frameworks where industry leads decisively by leveraging the mature assets and capabilities of ICT companies.

**Project Phases and Methodology.** The CSDE's work on industry responses to a cyber crisis builds on findings and recommendations in the November 19, 2014 National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Information and Communications Technology Mobilization<sup>12</sup> and the June 2016 Homeland Security Advisory Council Final Report of the Cybersecurity Subcommittee on Incident Response,<sup>13</sup> as well as similar calls to action in other jurisdictions, such as European Union Agency for Network and Information Security (ENISA) publications on cyber crisis cooperation.<sup>14</sup>

This report documents the CSDE's efforts to identify key resources among global ICT companies across two distinct phases.

- ▶ During the first phase, the CSDE identified categories of cyber threats and vulnerabilities that may require the mobilization of the ICT sector. These categories were chosen in consultation with experts and sources from industry, government, and civil society.
- ▶ In the second phase, the CSDE conducted a survey of member companies, leveraging the expertise of leading cybersecurity professionals and other institutional resources, to identify (1) incident response assets and capabilities that ICT stakeholders may provide to mitigate a crisis scenario and (2) potential industry responders in select crisis scenarios. *See Appendix A for the survey scenarios.*

Producing this guide reflects our broader commitment to reducing barriers to cooperation in cyber crises. We will share this guide with a broad set of stakeholders throughout the ecosystem and undertake concerted efforts to encourage participation by key trusted companies in incident response efforts for the security of our digital economy.



## 03 | Overview of Global ICT Segments Represented in the CSDE

**IN THIS SECTION**, we describe the different types of ICT companies that are represented in the CSDE's membership and are likely to be essential during one or more categories of potentially catastrophic cyber events. We recognize that all ICT companies, including those not described in this section, have a role to play in securing the global digital ecosystem against a range of cyber threats and vulnerabilities.

To the extent that the types of providers described in this section may not have all of the assets and capabilities needed to respond to a crisis, they will sometimes have formal or informal working relationships with other parties that can help mitigate the crisis.

**Infrastructure Providers.** The internet is a complex “system of systems” with many different layers of infrastructure that enable connectivity and operability. Represented among the CSDE's diverse membership are leading global ICT companies that provide the infrastructure that enables internet access and content delivery and, along with other stakeholders in the digital economy, their capabilities would likely be critical in mitigating specific types of cyber crisis scenarios.

### ***Internet Service Providers***

An internet service provider (ISP) is an organization that provides customers a means to access the internet using technologies such as cable, DSL (digital subscriber line), dial-up, and wireless. ISPs are connected to one another through network access points, public network facilities found on the internet backbone. ISPs use these vast systems of interconnected backbone components to transfer information across long distances within seconds. ISPs may provide services beyond accessing the internet including web-site hosting, domain name registration, virtual hosting, software packages, and e-mail accounts. Many ISPs offer a large variety of security solutions, including managed services, whereby the provider takes an active role in mitigating threats to their customers.

### ***Internet Backbone Providers***

The internet's backbone is a collection of vast, connected computer networks that are generally hosted by commercial, government, academic, and other network access points. These organizations typically have control over large high-speed networks and fiber optic trunk lines, which are essentially an assortment of fiber optic cables bundled together in order to increase capacity. They allow for faster data speeds and larger bandwidth over long distances, and they are immune to electromagnetic interference. Backbone providers supply ISPs with access to the internet and connect ISPs to one another, allowing ISPs to offer customers high speed internet access. The largest backbone providers are called “Tier 1” providers. These providers are not limited to country or region and have vast networks that connect countries across the world. Some Tier 1 backbone providers are also ISPs themselves and, due to their size, these organizations sell their services to smaller ISPs.

### ***DNS Providers***

The Domain Name System (DNS) is essentially an address book of domain names associated with IP addresses copied and stored on millions of servers around the world. When a user wishes to visit a website and types the domain name into the search bar, the computer sends that information to a DNS server. This server (also referred



to as a resolver) is usually run by the user's ISP. The resolver then matches the domain name with an IP address and sends the corresponding IP address back to the user's browser which then opens a connection with the webserver. DNS providers are organizations that offer such DNS resolution services. They provide the most common DNS functions such as domain translation, domain lookup, and DNS forwarding. DNS providers also routinely update their name servers to provide the most current information.

### ***Content Delivery Networks***

A content delivery (or distribution) network (CDN) is a geographically dispersed network of data centers and proxy servers. CDN is a term used to describe many different types of content delivery services such as: software downloads, web and mobile content acceleration, and video streaming. CDN vendors may also cross over into other industries like cybersecurity with DDoS protection and web application firewalls (WAF). CDNs were designed to solve a problem known as latency, the delay that occurs between the time that a user requests a web page to the moment that its content appears onscreen. The duration of the delay typically depends on the distance between the end user and the hosting server. To shorten this duration, CDNs reduce that physical distance and improve site rendering speed and performance by storing a cached version of its contents in several locations, known as points of presence or PoPs; each PoP connects end users within its proximity to caching servers responsible for content delivery. By storing a website's content in many places at once, a company can provide superior coverage to far away end users, while also providing an additional layer of security.

### ***Cloud and Hosting Providers***

Internet hosting services enable customers to make content accessible on the internet to people and organizations throughout the world. In recent years, the increased adoption of cloud hosting services, which use remote servers hosted online instead of a local server or a personal device, has given customers access to scalable and more secure hosting solutions. Software, infrastructure, and platforms hosted on the cloud can be accessed on a subscription basis and enable customers to perform a wide variety of computing functions. Because cloud networks are decentralized, they can typically withstand the disruption of numerous network components. This architectural feature makes the cloud more resilient to distributed cyber-attacks and provides additional mitigation capabilities. In essence, cloud services provide access to a wide range of content and functions, as well as an incremental layer of security, outside of the infrastructure provided by an ISP.

**Software Developers and Vendors.** Software is an increasingly ubiquitous element of the digital ecosystem. Accordingly, many types of software developers and vendors are represented in the CSDE. In the event of a cyber crisis, software developers and vendors may play multiple roles depending on the types of products and services they offer customers and the nature of the crisis, among other situation-specific considerations.

In general, software may be divided into systems and applications. Systems enable users to operate and manage hardware. Applications are programs that enable an incredibly wide range of computing functions. Every single day, millions of people download applications onto their personal smart phones and endpoint devices. Application software includes antivirus programs and other programs designed to improve security.

Components of software may be proprietary or open source. Proprietary software components have legal conditions on their use and their source code may be a closely guarded company secret, in order to protect the rights and

commercial interests of the owners. Open source software components, as the name implies, have a source code that is accessible to the general public, and it can be used or modified by any interested party with sufficient technical skills.

In some scenarios, developers of propriety software may have specific insights relevant to mitigating a security issue. Even if the issue stems from vulnerabilities in software components that no ICT company owns, a large software company's institutional knowledge and experience mitigating software-based risks may be beneficial to incident response and recovery efforts.

**Hardware Manufacturers and Vendors.** For purposes of this report, hardware refers to the tangible components of ICT systems, including devices as well as network equipment that connects systems across end users' homes or across the globe. The complexity and security considerations associated with hardware will vary greatly based on its intended use and relationship to software and network components of the ecosystem.

The CSDE's diverse membership includes original equipment manufacturers (OEMs) and hardware vendors. During a crisis that originates with a hardware-based vulnerability, the CSDE members that create hardware components may have important insights and mitigation capabilities.

Some manufacturers create hardware specifically for systems of devices. An individual connected device (or "endpoint device") may itself consist of multiple components, including hardware modules, chips, software, sensors or other operating components. Hundreds of thousands of companies and millions of developers potentially contribute to the billions of individual devices deployed throughout the world.

Other manufacturers create hardware for infrastructure or advanced industrial processes that increase efficiencies across numerous sectors of the global economy. Based on the criticality of the hardware in specific systems or process to ecosystem-wide priorities, different companies are likely to have varying levels of appropriate risk management capabilities.

**Security Service Providers.** Professional security services offer customers key advantages in the event of a crisis. The CSDE's membership includes Managed Security Service Providers (MSSPs) and Incident Response Service Providers.

Managed Security Service Providers (MSSPs) offer remote IT management and monitoring services for their customers, either complementing in-house security teams or providing broad sets of security solutions. MSSPs serve many different markets including large companies, governments, nonprofits, and small and medium-sized business, among others. Services offered by MSSPs may include services such as intrusion detection and filtering solutions (e.g., firewalls), as well as unified threat management. A number of CSDE members offer fully managed end-to-end solutions to increase network security. MSSPs may offer some services that help mitigate cyber-attacks known to compromise large organizations, for example data breaches and ransomware, as well recover from those types of incidents.

Incident Response Service Providers help customers respond to an incident with the goal of reducing damage and exposure. They use threat intelligence to help customers make decisions during a crisis and develop custom strategies to identify the attacker and get to the root cause of an incident. Incident Response Service Providers are typically hired on a retainer. Because time and geographic presence are of the essence during a crisis, providers may have the capability to assist customers remotely while traveling to their physical locations.

## 04 | Private Sector Cyber Crisis Assets and Capabilities

**COMMERCIAL OFFERINGS** in the global ICT ecosystem are highly complex and dynamic. Companies across the world will evolve their business models, services, and products — and therefore their role within the ecosystem — based on market incentives, competition, technological evolution and convergence, and opportunities for innovation, among other considerations that lead to new strategies for delivering value to different sets of customers.

In recent years, technological advances such as cloud migration have led to increased convergence between the technological capabilities of different types of service providers, manufacturers, developers, and vendors whose offerings depend on shared resources and functionality. Previously unrelated technologies are now closely linked via underlying digital platforms enabled by diverse connective infrastructure. It is a well-observed tendency that, over time, technologies tend to become increasingly interoperable to expand their functions, security, and efficiency, akin to how biological systems evolve and adapt in response to their environments.

This section offers a snapshot of the assets and capabilities that leading ICT companies may have during a crisis, if a catastrophic incident were to occur today. In the event of a crisis, the assets and capabilities of different companies could overlap to varying extents. For example, leading ISPs offer customers some of the same services as security vendors. Companies that sell and manufacture hardware for systems and devices may also develop software components. Providers of Industrial Control Systems (ICS), for instance, incorporate software, firmware, hardware, and network components.

In order for governments to determine the most relevant, leverageable assets and capabilities of any given company, they should build close working relationships with the companies whose leadership and experience in responding to high-level cyber incidents makes them valuable partners in the global fight against cyber threats.

All types of ICT companies must be vigilant of unique security concerns affecting their constituencies across relevant segments of the digital ecosystem. The assets and capabilities of ICT companies during catastrophic cyber events generally include the following security teams and professionals:

- ▶ **Threat Intelligence Sharing Partnerships**
- ▶ **IP Network Operations Center (IP NOC)**
- ▶ **Security Operations Center (SOC)**
- ▶ **Computer Security Incident Response Team (CSIRT)**
- ▶ **Product Security Incident Response Team (PSIRT)**
- ▶ **Cybersecurity Vulnerability Assessors**
- ▶ **Security Engineers and Other Cybersecurity Professionals**
- ▶ **Subject Matter Experts**

**Roles of Security Teams in a Cyber Crisis.** As primary drivers of technological innovation and progress across the globe, leading ICT companies collectively have at their disposal some of the world's most advanced cybersecurity and incident response assets; these range from state-of-the-art operations facilities with sophisticated mitigation tools, technologies, and processes to experienced teams of cybersecurity experts who are qualified to handle crisis-level events.

Given the vast array of global companies and institutional cultures in the digital ecosystem, these assets and their associated capabilities can be implemented differently by individual organizations and may be referred to by diverse names within each organization. Nonetheless, they share key functions and operational structures in common that make them recognizable across a variety of nomenclatures.

The following is not intended to be a comprehensive listing of ICT assets and capabilities, but rather an executive overview of high-value resources for mitigating cybersecurity incidents that, absent rapid and effective mitigation, could have devastating consequences for public safety, security of nations across the world, and the global digital economy.



### ***Threat Intelligence Sharing Partnerships***

Threat intelligence sharing partnerships across the cybersecurity community facilitate the exchange of vital threat intelligence with both public and private sector partners, and with governmental agencies around the globe. Partners may share critical non-public indicators — such as malicious IP addresses and domain names, malware used in attacks, and unique tactics used by advanced threat actors — to better protect clients, partners and the public. While no single organization, public or private, has complete visibility into the threat landscape, the breadth of visibility by the largest ICT companies is compelling. Further these same companies arguably have the most extensive range of information-sharing relationships. The individual and collective visibility of these companies provides the means to fill in gaps in both regional and global visibility and collaborate in real-time — thereby enabling threat responders to more quickly and effectively remediate threats.

### ***IP Network Operations Center (IP NOC)***

An IP NOC is a facility designed to enable management of an IP network to preserve infrastructure integrity and functionality, minimize service disruptions and downtime which may be caused by cyber incidents, and meet the requirements of service-level- agreements. The IP NOC provides situational awareness of the network's traffic and performance on an ongoing basis through monitoring and analysis.

The facility may have large screens that display visual representations of the network's status and operations. The IP NOC will typically be staffed by human operators, such as security engineers, who are well-trained at interpreting the data traveling through the network and may receive notifications from customers or other parties about disruptions or anomalous activity. The IP NOC may also be able to contact customers in case of an emergency.

Global infrastructure providers' IP NOCs have at their disposal systems and applications necessary to perform traffic management; assist customers or peers with troubleshooting; distribute software updates; and manage infrastructure such as servers, routers, and domain names.<sup>15</sup>

### ***Security Operations Center (SOC)***

An SOC is the central team within an organization responsible for cybersecurity. It oversees the human and technological processes and operations necessary to defend against cyber threats. An SOC's functions may include all categories of activities identified in the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.<sup>16</sup>

SOCs of large companies may be comprised of multiple teams, each equipped with a specialty that complements the others. These groups can work in tandem to respond to large-scale cyber incidents. A Command SOC team may be designated to coordinate the actions of other teams. Some teams may function autonomously for strategic purposes.

In the case of large companies, the SOC will typically have at least one physical headquarters or facility with specialized equipment that allows the team to carry out its mission. For example, an SOC can monitor and analyze network activity, including in the cloud, as well as endpoints, applications, and connected systems, in order to provide a source of intelligence to identify security incidents.



In addition to helping identify security incidents, some SOC's have advanced capabilities such as digital forensics and reverse-engineering, which allow them to analyze a threat in-depth and provide valuable intelligence to combat cyber threats.

In a cyber crisis, the primary focus of a Command SOC team is to quickly activate the relevant Computer Security Incident Response Team (CSIRT) (see below) to respond to the incident's specifics and, when appropriate, stand-down the response team as quickly as possible to return to business as usual. The Command SOC is also the entity that generally determines when to contact parties outside the company. Typically, the response team will only be activated during a significant cyber-attack or large-scale cyber incident.

### ***Computer Security Incident Response Team (CSIRT)***

This team is activated only during critical cyber-attacks or vulnerabilities and often employs a structure that is compatible with recognized best practices that enable a company to swiftly take action during crisis events. The role of the CSIRT is to limit damage, facilitate recovery efforts, and take steps to mitigate against future incidents. The human element of a CSIRT are security experts who can coordinate incident response across an array of different cyber incidents determined by the needs of the organization and its constituencies.

CSIRT staff may be trained to handle situations that could lead to potentially catastrophic incidents for public safety and national security. The CSIRT will have specialized knowledge of the threats facing the company and its customers, as well as response strategies tailored to the company's resources and priorities during a cyber crisis.

CSIRT strategies for responding to cyber crises evolve along with technology and may be updated regularly, shared with team members, and tested often throughout the year in table top and simulation exercises. Strategic considerations for large companies include the people, processes, and tooling required for the team to respond to heightened levels of cybersecurity incidents.

### ***Product Security Incident Response Team (PSIRT)***

A Product Security Incident Response Team (PSIRT) is an entity within an organization that focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components, and/or services which an organization produces and/or sells.<sup>17</sup> Software and hardware vendors' PSIRTs are the teams that coordinate the disclosure of those vulnerabilities to their customers.

### ***Cybersecurity Vulnerability Assessors***

A cybersecurity vulnerability assessment (CVA) is an in-depth analysis of an organization's security posture conducted by experts who are trained to discover actual or possible exposure to cyber threats. By conducting CVAs, an organization can make informed decisions about how to mitigate risk and manage resources cost-effectively in order to prioritize the most serious types of threats. CVAs may assess the attack surfaces of networks, devices, systems and application software, and other ICT assets. These capabilities help security leaders identify and remediate security flaws, covering their entire digital and physical ecosystem.

Companies may have the capability to conduct CVAs in-house or they may contract with third parties to obtain these services. Penetration testing, a feature of some assessments, is generally carried out by autonomous teams

of experienced hackers hired to break into organizations and uncover risky vulnerabilities that threat actors may take advantage of. Similarly, Red Team assessments involve hiring hackers to break into an organization, but often more closely mirroring a real-world situation, where the goal is to get in by any means necessary, rather than to uncover the greatest number of vulnerabilities. In general, the hired hackers can do what criminal hackers can do, but with the goal of helping security leaders harden their defenses and protect their most important assets.

### ***Security Engineers and Other Cybersecurity Professionals***

Security engineers are cybersecurity professionals whose job is to protect and mitigate against cyber threats. This is an advanced-level job according to the CyberSeek model developed by the National Initiative for Cybersecurity Education (NICE), a partnership led by NIST between government, industry, and academia to promote cybersecurity workforce development.<sup>18</sup> Security engineers are often on the front lines during a cyber-attack against global ICT companies. For example, network security engineers have essential skills for resolving issues such as DDoS attacks and BGP hijacking.

Many cybersecurity professionals in the employ of ICT companies have skills and knowledge that may be leveraged during cybersecurity events. The CyberSeek model provides a comprehensive overview of the different types of cybersecurity professionals.<sup>19</sup> The individuals employed or contracted to these companies will clearly align with that company's products, services or needs.

### ***Subject Matter Experts (SMEs)***

In responding to cyber incidents, companies may leverage input from experts (either in-house or external to the organization) that are recognized for their specialized knowledge in relevant fields of cybersecurity. For example, an ISP may leverage the knowledge of an in-house DNS expert to ensure proper configuration of domain names. When dealing with newly discovered hardware or software vulnerabilities, a vendor may consult leading security researchers. As technology grows more complex, we will likely continue to see greater degrees of specialization among experts.

Technical experts aside, other types of SMEs will likely provide input before finalizing courses of action. Considerations such as privacy, legal and regulatory considerations, business operations, communications with customers, collaboration with governments across the globe, and other subjects may be relevant to incident response.

## 05 | Public-Private Coordination in Cyber Crisis Scenarios

**AS A MAJOR VOICE** of global ICT companies, the CSDE can play a leading role in promoting collaboration among industry and government to prepare for cyber crises. In addition, we can work with governments and industrial bodies to harmonize international frameworks.

**Events Prior to Joint Cyber Crisis Response.** As a matter of course, information-sharing is ongoing among and between these companies. The laws and policies governing information-sharing procedures for cyber threats can vary from country to country. Nonetheless, global efforts are currently underway among like-minded governments to increase information-sharing.<sup>20</sup>

Enterprises must collaborate within their own sectors and with government to share knowledge of pertinent cyber threats. Indeed, enterprises are often the first to discover a cyber threat because their systems are directly impacted when an incident occurs. Due to their unique positions in the cyber ecosystem, they have a capability to alert industry and government when a serious incident occurs and share critical information needed to recognize emerging threat patterns in the ecosystem.<sup>21</sup> Generally, large enterprises have more access to the institutional knowledge, technical training, and other resources needed to collaborate effectively with industry and government. However, smaller enterprises in the aggregate can also contribute to evidence of emerging cyber threat patterns.<sup>22</sup>

In many countries, enterprises can share information with an Information Sharing Analysis Center (ISAC) or functional equivalent.<sup>23</sup> The ISAC or its equivalent can then share the information with trust groups to the extent permitted by each country's laws. At this stage, a determination must be made whether the incident is serious enough to merit the involvement of leading ICT companies.

**Considerations in Supporting Joint Cyber Response.** Ultimately, each company must decide when and how to deploy assets and capabilities it considers appropriate to mitigate a cybersecurity incident, and the extent to which the company will either request assistance or provide assistance to others. This decision is made using a multi-factored analysis, which can include policy and legal considerations, as well as practical realities on the front lines of cyber-defense. Once acting in collaboration with other ICT partners, some companies voluntarily adopt industry protocols that help guide multi-party operationalization in a crisis. For example, a number of CSDE members are charter members of ICASI, which developed the *Unified Security Incident Response Plan* (USIRP).

Companies' decisions may be informed by diverse opinions from experts in multiple countries, and while there is no single definition of a cyber crisis that will apply in every scenario, a number of helpful considerations have been identified by experts.

For example, the NSTAC report calls for leading ICT companies to be mobilized in "widespread" or "particularly grave" events.<sup>24</sup> A widespread event can mean "complete infiltration of a sector or substantial foothold across two or more sectors."<sup>25</sup> A grave event can mean "a critical dependency is completely overwhelmed and request for resources exceeds available capabilities."<sup>26</sup>

Similar concepts are found in the incident response strategies of other jurisdictions. ENISA's *Strategies for Incident Response and Cyber Crisis Cooperation* defines a crisis as “an extraordinary event that differs from the normal and involves serious disturbance or risk for disturbance of vital societal functions”; “an abnormal and unstable situation that threatens an organisation’s strategic objectives, reputation or viability”; and an “event that strikes at the heart of the organization”.<sup>27</sup>

Appendix A contains twelve (12) scenarios identified by the CSDE that could escalate to a scale that causes a number of ICT companies to take coordinated action against a common threat. These scenarios are based on the following types of cyber incidents:

- ▶ **DDoS Botnet Attack**
- ▶ **DDoS Server-based Attack**
- ▶ **Border Gateway Protocol (BGP) Hijacking**
- ▶ **Domain Name System (DNS) Hijacking**
- ▶ **Software Vulnerabilities: Open Source**
- ▶ **Software Vulnerabilities: Zero Day**
- ▶ **Hardware Vulnerabilities: Processor Architectures**
- ▶ **Injection of Malicious Code in Software and Hardware Components**
- ▶ **Destructive Malware**
- ▶ **Ransomware**
- ▶ **Advanced Persistent Threat (APT): Industrial Systems**
- ▶ **Cloud Provider Compromise**

**Roles of ICT Companies During Cyber Crises.** When a cyber threat or vulnerability presents itself, the relevant ICT companies can self-select into groups capable of rapidly mobilizing critical private sector assets to effectively respond in the event of a major cyber emergency. To the extent practical, industry response strategies may be pre-coordinated while recognizing the evolving and dynamic nature of the threat.

Based on an extensive survey of CSDE members, we developed an understating of the likely roles of different ICT segments in each of the scenarios analyzed. This understanding is represented below and, although subject to changes based on the situational realities “on the ground” during an incident, should serve as effective general guidance for private and public ICT stakeholders.

In addition, major companies represented in the CSDE, even if not directly relevant to a resolving a security issue, may be able to help government or industry partners quickly identify relevant ICT companies (infrastructure, software, hardware, security service providers, and others) in the initial triage stage of a potential or actual crisis, in order to facilitate and expedite critical response efforts. Further, these same companies may be in the best position to provide meaningful support in implementing the joint response.

### DDoS Attacks

- ▶ **Scenarios Examined:** DDoS Botnet Attack; DDoS Server-based Attack
- ▶ **Potential Responders:** Situationally relevant Infrastructure Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers

### Internet Traffic Hijacking

- ▶ **Scenarios Examined:** Border Gateway Protocol (BGP) Hijacking; Domain Name System (DNS) Hijacking
- ▶ **Potential Responders for BGP Hijacking:** Situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors; Managed Security Service Providers
- ▶ **Potential Responders for DNS Hijacking:** DNS Providers; situationally relevant Infrastructure Providers; Networking Hardware, Software, and Systems Vendors

### Software Vulnerabilities

- ▶ **Scenarios Examined:** Open Source Vulnerabilities; Zero Day Vulnerabilities
- ▶ **Potential Responders:** Situationally relevant Software Vendors; Original Software Developers (OSDs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

### Hardware Vulnerabilities

- ▶ **Scenarios Examined:** Processor or Component Vulnerabilities
- ▶ **Potential Responders:** Situationally relevant Hardware Vendors; Original Equipment Manufacturers (OEMs); Operating Systems and Firmware Vendors; Virtualization Vendors; Cloud and Hosting Providers; Managed Security Service Providers

### Software and Hardware Component Backdoors

- ▶ **Scenarios Examined:** Injection of Malicious Code in Software and Hardware Components
- ▶ **Potential Responders:** Same potential responders as Software and Hardware Vulnerabilities respectively

### Malware and Ransomware

- ▶ **Scenarios Examined:** Destructive Malware; Ransomware
- ▶ **Potential Responders:** Situationally relevant Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers

### Advanced Persistent Threats (APTs) and Cloud Compromises

- ▶ **Scenarios Examined:** Advanced Persistent Threat (APT): Industrial Systems; Cloud Provider Compromise
- ▶ **Potential Responders:** Cloud and Hosting Providers; Software Vendors; Hardware Vendors; Managed Security Service Providers; Incident Response Service Providers



### **Advance Planning for Joint Cyber Response:**

The scenarios highlighted above occur on a regular basis, albeit at a smaller scale not requiring the level of mobilization contemplated within this report. These smaller-scale events provided the insights into the likely class of responders that might be required under more extreme circumstances. What these scenarios cannot tease out with any precise definition is the specific names of the companies within these categories that might be situationally relevant for any given event. Below, we look at two examples and expand on the escalation process that might lead to a Joint Cyber Response.

#### ***Example: Mitigating Software and Hardware Vulnerabilities***

Recent developments such as the exponential growth of connectivity have shown the world that a vulnerability in either software or hardware components can have significant consequences that reverberate throughout the digital ecosystem. A single security flaw in a piece of code or hardware component can potentially impact a wide range of products. While coordination efforts are notionally the same for software and hardware ICT components, mitigating hardware vulnerabilities can require considerable multi-party coordination and may present operational challenges that are unique to the hardware context. The multi-party coordination effort for a vulnerability in a technology owned and manufactured by the vendor leading the process might entail different processes than one in which a broader collaboration is needed and there is no one distinct owner/manufacture of the technology (e.g., protocol-level vulnerabilities).

Responding to incidents involving vulnerable ICT components or software, whether in device systems or infrastructure, may require an understanding of factors such as how hardware and software components and systems are integrated and the environment in which components are deployed. For example, software companies including operating systems and firmware vendors and virtualization vendors may be integral to the process of developing and testing a mitigation for a hardware-based vulnerability (in a process often termed “Multi-Party CVD”, led by the hardware manufacturer). Cloud providers also play an important role in mitigation development and testing for infrastructure they operate.

Four of the scenarios outlined above fall predominantly in the Software/Hardware domains: Software Vulnerabilities-Open Source, Software Vulnerabilities-Zero Day, Hardware Vulnerabilities-Processor Architectures, and Injection of Malicious Code in Software and Hardware Components.

In the case of a Hardware Vulnerability, usually the Hardware Company manufacturing the component, technically knowledgeable of the product, is best situated to lead the coordination effort. Relevant ecosystem partners collaborating with the hardware manufacturer in the Multi-Party coordination effort will also likely be situationally relevant and take part in the mitigation development and testing effort, as needed. Such parties may include other manufacturers of directly-affected hardware products (if applicable), vendors involved in assembling the product into different systems and products (OEMs) or partners integrating the components in certain technical environments that require further consideration (e.g., operating system, cloud environments, software and firmware development). Please note: the vast majority of cyber incidents in this context are addressed, and mitigations are developed, as part of a Multi-Party CVD process led by the hardware manufacturer in collaboration with the Vendor/Partner ecosystem.

In other, different, Multi-Party CVD settings (software or hardware) in which there is no clear owner of the technology/manufacture best-situated to lead the coordination efforts (for example, in certain protocol-level vulnerabilities),

and depending on the nature of the attack, a broader collaboration within the ecosystem may be needed to develop, test, and release mitigations. In this stage, ICT companies may consider reaching out to like-companies to explore if they (or their partner ecosystems) have insights into mitigation or containment strategies in a Multi-Party CVD effort encompassing a broader set of representatives from the technological ecosystem. Such outreach might extend to entities like ISACs/ISAOs or other comparable venues.

The need to mobilize peer (and potentially competitor) hardware/software companies to address and mitigate events is already understood, and protocols to do so have been proposed and are already in place.

For example, a number of CSDE members are charter members of ICASI, which developed the *Unified Security Incident Response Plan* (USIRP). The Unified Security Incident Response Plan (USIRP) is one of the primary means by which ICASI fulfills its mission of enhancing the global security landscape. Comprising a trusted forum and supporting processes, procedures, and tools, the USIRP enables Security Incident Response Teams (SIRTs) from ICASI member companies as well as select, invited outside organizations to collaborate quickly and effectively to resolve complex, multi-stakeholder Internet security issues (such as in protocols)<sup>28</sup> in which there is no clear one owner/manufacturer leading the coordination effort and broader collaboration is needed.

Some of the types of issues addressed in this environment are reflected below:

### COORDINATED VULNERABILITY DISCLOSURE (CVD)

CSDE's member companies, together with security researchers in many countries across the world, are working constantly to discover and address vulnerabilities in technology (software, firmware, hardware) and develop protective measures to mitigate against the risks posed by those and other vulnerabilities. The globally intertwined nature of technology and international collaboration that CVD and Multi-Party CVD entails supports the development, adoption and harmonization of consensus-driven international best practices and standards that align and are informed by industry best practices.<sup>29</sup>

The complexity of ICT components and software that are essential to the digital economy, as well as the security of nations and global infrastructure, creates incentives for trusted researchers in the cybersecurity community to collaborate across sectors and often with government partners. At the same time, companies from all sectors have a responsibility to carefully limit the spread of information concerning the vulnerability that could be misused by malicious actors to create harm while mitigations are not available.

ICT components and software may have security vulnerabilities that expose systems to risk, which may result in economic and national security challenges. To address these challenges, as well as more mundane security vulnerabilities, the process known as CVD has emerged to minimize harm to the global community. In the past, CVD was focused on software and software-based products. But the rapid transformation of the digital ecosystem, among other security-related developments, has led to increased development on hardware vulnerability and Multi-Party CVD disclosure best practices.

The security rationale for CVD is commonsensical: disclosing vulnerabilities before mitigations are ready and available for end users makes exploitation more probable. To reduce the likelihood of widespread exploitation, CVD limits disclosure of vulnerabilities at each step to those stakeholders that are essential contributors to mitigation. At the same time, the CVD process seeks to promote reasonably fast-paced development of mitigations and strategies to distribute those mitigations effectively.

The CVD process guides vendors, security researchers, and other stakeholders in the digital economy to cooperate on the development of mitigations addressing a given vulnerability while simultaneously limiting disclosure of information concerning that vulnerability until such time as mitigations and information can be made available to the public in a coordinated manner.<sup>30</sup> The CVD process is consistent with NIST's Cybersecurity Framework, which recommends the establishment of processes to "receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)."<sup>31</sup> The National Telecommunications and Information Administration (NTIA) has collaborated with industry and global stakeholders represented in the Forum of Incident Response and Security Teams (FIRST) to develop guidelines and practices for multi-party vulnerability coordination and disclosure.<sup>32</sup> There are also widely-adopted international standards focusing on Coordinated Vulnerability Handling and Disclosure, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018).

During incident response, time is often of the essence. Sometimes, patching hardware vulnerabilities can be very complex, requiring collaboration and complex coordination between multiple vendors (a process often referred to as "Multi-Party CVD") to develop and test mitigations and deliver them to end users.<sup>33</sup> In some cases, various approaches to mitigation based on respective architectures are considered. This was the case, for example, of the Spectre and Meltdown exploits which took advantage of a common feature in modern processors (while being relatively difficult to exploit). In some cases, it may be appropriate to deploy temporary workarounds until more enduring fixes and mitigations are available. Over time, even very complicated challenges can often be solved but may require a longer period of time for coordination in complex environments.<sup>34</sup>

If a significant cyber-attack occurs before appropriate mitigations are ready, stakeholders may disclose information and guidance necessary to minimize harm to the public, while withholding information that bad actors could use to make the situation worse. This is a careful balancing act and requires careful coordination among the relevant parties. Intermediaries such as national CERTs can sometimes help stakeholders in the CVD process cooperate effectively on shared security goals.

## SOFTWARE AND HARDWARE MITIGATIONS DISTRIBUTION

In the case of software vulnerabilities, mitigations distribution may require nothing more from a technical perspective than updating the relevant code libraries. Often, the bigger challenge is persuading users or other properly authorized decision-makers to accept updates in a timely and coordinated manner. Mitigating hardware vulnerabilities, however, may require coordination among manufacturers, suppliers, technicians, and vendors that fill distinct roles necessary to secure the hardware components of a system.

On the one hand, there are easy updates on smart phones and computers that users are familiar with, as well as hassle-free software as a service (SAAS) updates in the cloud environment. On the other hand, many IoT devices would need physical upgrades that are commercially unfeasible and, in some cases, may cost more to deploy than the device is worth. This is why it is important to design devices securely in the first place. The CSDE's *International Anti-Botnet Guide* provides relevant guidance on secure-by-design development and mitigations strategies for device systems. In addition, the CSDE C2 Consensus on IoT Device Baseline Security is the broadest and most technically deep industry consensus on IoT security worldwide. You can download these documents on our official website: [securingdigitaleconomy.org](https://securingdigitaleconomy.org).

An important factor in a hardware component manufacturer's capability to distribute mitigations is how the component is integrated into device systems or infrastructure. A component vendor that has no direct relationship with the customers who own device systems or infrastructure will probably collaborate with additional stakeholders (like OS vendors and OEMs) to distribute mitigations to end users. A vendor that produces all components for a device — for example, a simple IoT device or industrial control system (ICS) — may in some circumstances have the ability to handle the distribution on its own.

Because of complexities in distribution of hardware mitigations, the timeframe will vary on a case-by-case basis,<sup>34</sup> and pressures may increase on stakeholders to disclose vulnerabilities. However, in the interest of protecting the public against widespread threats before mitigations are available, the CVD process should be followed and the information should be kept in confidence.

### **DISTINGUISHING SOFTWARE AND HARDWARE VULNERABILITIES VS. BACKDOORS**

Software and hardware vulnerabilities, like other security vulnerabilities, are unintended and often result from human error or technical complexities. In contrast, backdoors are intentionally created by sophisticated cyber adversaries. A full discussion of cyber supply chain security and policy issues is outside the scope of this report. However, certain principles of coordinated vulnerability disclosure may be adapted in the context of more comprehensive supply chain risk management strategies, as determined by each organization's policy as well as legal considerations. Moreover, we recognize that mitigating backdoors presents some of the same sets of mitigation distribution challenges as unintended vulnerabilities, and therefore many of the same solutions in most cases.

#### ***Example: Mitigating Cyber Threats Related to Internet Traffic***

Significant cybersecurity incidents involving internet traffic and its contents arise when traffic is harnessed for destructive ends, such as in the case of distributed denial of service (DDoS) attacks, and when traffic is improperly redirected or "hijacked" by malicious actors, such as during BGP and DNS hijacking attacks.

Four of the scenarios outlined above fall predominantly in the domains associated with mitigating threats related to the internet traffic: DDoS Botnet Attack, DDoS Server-based Attack, Border Gateway Protocol (BGP) Hijacking, and Domain Name System (DNS) Hijacking

Preventing DDoS Attacks is a shared responsibility among all stakeholders in the digital economy. In recent years, some of the most damaging DDoS attacks have involved botnets — large networks of compromised endpoints such as computers and devices — that took advantage of weak security features in Internet of Things (IoT) devices, as exemplified by the notorious Mirai botnet attack in October 2016, and have been a source of global concern ever since. And, indeed, CSDE membership includes some providers of state-of-the-art commercial DDoS mitigation services. Combating these and other automated, distributed threats has been a major goal of the CSDE, which is why in 2018 we released the *International Anti-Botnet Guide*. You can download the Guide at [securingdigitaleconomy.org](https://securingdigitaleconomy.org).

Mitigating DDoS attacks is largely handled by the Infrastructure Providers, who can act on behalf of the customers under attack. DDoS attacks are generally targeted at an end user or class of users, with the intent being to disrupt the ability of the user(s) to access their services.

In the case of mitigating DDoS attacks, the most situationally relevant player will be the underlying service provider for the user being attacked, but DDoS resolution brings in other infrastructure such as (1) the infrastructure provider of the originating attacker, (2) hosting providers/data centers, (3) content delivery networks, and (4) the multiple providers of infrastructure upon which the attack traffic travels. While the specific infrastructure provider(s) implicated in the DDoS event cannot be anticipated in advance, the Tier 1 backbone providers are minimally in a support role.

These infrastructure providers have a variety of DDoS mitigation techniques that can be used to address the issue including (1) blackholing traffic targeted towards the IP address under attack, (2) selective blackholing, which changes the BGP routing for the targeted address so that it is only from certain parts of the internet, and (3) traffic scrubbing, where the infrastructure provider redirects traffic to the targeted IP range to a scrubbing center, which scrubs the unwanted attack traffic and returns the normal traffic. There are additional network engineering and local filtering techniques which can also be used.

While the Infrastructure Provider group does not have an organization comparable to ICASI highlighted above, the connection, interconnection and peering relationships between these infrastructure provider classes are exercised daily in addressing traffic anomalies and threats.

Issues arising from internet traffic hijacking through BGP or DNS vulnerabilities are handled in a comparable fashion. Global ICT companies, in particular internet infrastructure providers (e.g., ISPs, backbone providers, DNS providers, CDNs, and providers of cloud-based infrastructure), have a variety of assets associated with internet traffic management. When internet traffic is wrongfully redirected, there are steps these companies may be able to take to remediate the situation, depending on factors such as who owns the assets responsible for the redirection and the relationship of each company to the affected parties, among other important considerations.

**Focusing on these two clusters of threats** provides insights into how the ICT companies choose to collaborate with either their immediate ecosystem, their extended community, or those companies outside this community. Companies leverage their own operational response protocols in collaborative initiatives. While similar in approach, these ICT companies have developed practices and protocols optimized to meeting their needs and their customers. Nonetheless, as the number of companies supporting an event expand, each one of these companies conducts a “triage” to determine who specifically (individuals/teams) within their company will work with these external players, and it’s usually only those individuals/teams that can contribute to a “solution” that are engaged. The “contribution” of company resources into any joint effort is meant to focus on resolving the issue at hand, somewhat akin to a SWAT team, and this work is consistently done on a virtual (and not physical) basis. Once a mitigation is developed, members of the virtual SWAT team convey progress and identify potential solutions to their respective companies for concurrence. Once a course of action is decided upon, the individual companies leverage their resources to implement the solution. Consistent with a unified course of action and unified messaging, the individual companies deploy those solutions using their own protocols, processes, and personnel.



Further, as outlined in the representative examples, determining which company is situationally relevant is dependent upon the event and the circumstances of the event. This report has identified the types of companies that will likely be implicated, but the specific name of the company that might be engaged is situationally dependent. Nonetheless, given their extensive global connections, the CSDE members are likely to assist in identifying which parties are the most situationally relevant and may be able to provide some support if the capacities of the identified companies are surpassed.

While there have been no events requiring a large-scale mobilization of ICT players across the ecosystem, smaller-scale events do provide an ongoing opportunity for the Infrastructure Providers as well as the Hardware/Software providers to engage with each other. Further, the companies represented within the CSDE use high-consequence exercises such as the CyberStorm and National Level Exercises to practice recognizing who the relevant players are, contacting and coordinating with those players, and developing a joint course of action. The work among industry players will continue, and the NLE 2020 series of exercises is the next major opportunity to do so.

Throughout the course of developing this report, a number of planning factors became clear: Effective incident response requires leveraging the different skill sets of diverse players, and no standard plan or protocol will accommodate every type of crisis. As demonstrated, combating malicious internet traffic, for instance, involves vastly different strategic security considerations, operations, and procedures than mitigating component vulnerabilities. Nonetheless, when CSDE members engage in incident response activities, they aim for common objectives: protecting people, nations, and economies against the worst consequences of significant cyber incidents and decreasing the likelihood of further escalation.



## 06 | International Coordination

**IN RECENT YEARS**, policymakers throughout the world have recognized the need for international cooperation and coordination to address the growing epidemic of cyber-attacks, particularly those that can rise to the level of a catastrophe.

For example, the NSTAC report states that “[a]t the levels contemplated, any ICT mobilization truly becomes an international undertaking with global implications and consequences, given the interconnected nature of the cyber ecosystem, the global distribution of cyber ecosystem functions and capabilities, and the decentralized operations of cyber bad actors. Consequently, successful cyber response must be a multi-stakeholder, multi-jurisdictional endeavor.”<sup>35</sup>

The European Union Agency for Network and Information Security (ENISA) stated: “The cross-border nature of threats and the associated mitigation mechanisms make it essential to focus on strong international cooperation. This requires major efforts at national level, at pan-European level and globally. There needs to be close cooperation with international partners to prevent and to respond to cyber incidents.”<sup>36</sup>

The CSDE’s membership, as stewards of a global digitally connected ecosystem, are encouraged by the increasingly widespread acknowledgement that in times of cyber crisis the ability to engage in multi-stakeholder and multi-jurisdictional collaboration is a necessity.

**The Need for Global Industry Leadership.** A cyber crisis requires immediate multi-jurisdictional collaboration. We cannot afford to waste time with first-time introductions when a power plant has stopped working, a financial system has been disrupted, or people lose access to healthcare services. The response in these kinds of situations must be swift and well-orchestrated.

While individual governments and enterprises take steps to protect their own systems from cyber threats, these systems are built upon the infrastructure, products and services of companies reflected within the CSDE membership. Moreover, these major ICT companies are global in nature and have experience combating a broad variety of cyber threats that spread rapidly from one jurisdiction to another.

By contrast, government and enterprise system managers have different levels of operational capability and institutional knowledge, different definitions for key concepts and terminology, and different relationships with the private sector and other relevant stakeholders — all of which can result in very delayed responses during a crisis, where time is of the essence.

Even when governments want to cooperate, they often struggle when dealing directly with foreign governmental entities due to a variety of reasons, including institutional norms, operational and legal obstacles, and lack of direct familiarity or established trusting relationships with people in other governments. Under these circumstances, leveraging the major ICT player relationships, even if their products and services are not immediately relevant, can provide connections and insights into which companies will likely be in the best position to mitigate the impacts of the specific event.

On the other hand, government authorities, like subpoena power or other investigative powers may be useful when seeking the cooperation of data center operators, foreign government officials, and other key players. Governments tend to have familiarity and established relationships with the private companies that operate in their respective jurisdictions. These companies also have key relationships with governments, private stakeholders, and other parties that can be assets during a crisis. By leveraging the private sector's distinct capabilities and relationships on a voluntary and mutually beneficial basis, governments can achieve their goal of a secure digital ecosystem through the leadership of global ICT companies.

## 07 | Next Steps

**THE CSDE CONSIDERED** the global stakeholder community when developing this voluntary guide that can be deployed across numerous jurisdictions and diverse legal environments. The CSDE's industry-led approach enables critical private sector assets to be leveraged in many parts of the world for incident response purposes.

As evidenced by the CSDE C2 Consensus on IoT Device Baseline Security, where the CSDE convened 19 associations from across the ICT sector to solve a common problem, we are well-positioned to develop operational and policy guidance that will be essential for shaping, enhancing, and promoting incident response capabilities.

By strengthening the relationships among key stakeholders, as well as developing guides to mitigate specific kinds of cyber threats and vulnerabilities, the CSDE will continue to serve as a critical forum for cyber policy leaders representing global ICT companies that are on the front lines during cyber-attacks and are committed to securing the digital economy.

## 08 | Appendix A: Cyber Crisis Scenarios Examined by CSDE

THE FOLLOWING SCENARIOS involve categories of cyber crises that could rise to the level of major disruptions of the global internet and communications ecosystem. These scenarios were chosen by CSDE members in close coordination with industry and government stakeholders.

- ▶ **DDoS Botnet Attack** — Malware infects a large number of devices to create a massive botnet and launch DDoS attacks against high value targets.
- ▶ **DDoS Server-based Attack** — An attacker exploits the vulnerabilities in servers to launch hugely amplified DDoS attacks.
- ▶ **Border Gateway Protocol (BGP) Hijacking** — A BGP hijacking attack wrongfully redirects internet traffic and may cause disruptions to websites and online services while also enabling attackers to steal data, conduct espionage, and perpetrate other abuses.
- ▶ **Domain Name System (DNS) Hijacking** — Malicious actors alter information on a DNS server to redirect internet traffic to the wrong online destination, such as a fraudulent website that misleads the public.
- ▶ **Software Vulnerabilities: Open Source** — Malicious actors discover security vulnerabilities in open source software components, which are used in commercial applications that proliferate widely throughout the internet ecosystem.
- ▶ **Software Vulnerabilities: Zero-Day** — Malicious actors discover software zero-day security vulnerabilities — vulnerabilities that software developers do not know about — and write exploit codes to gain unauthorized control and impair the functions of information systems all over the world.
- ▶ **Hardware Vulnerabilities: Processor Architectures** — A processor manufacturer identifies and discloses a vulnerability to a restricted set of ecosystem partners whose involvement in the coordination efforts is necessary for the vulnerability mitigation development and validation efforts.
- ▶ **Injection of Malicious Code in Software and Hardware Components** — A state-sponsored bad actor manages to insert malicious code into the software or hardware of major ICT companies, compromising systems in industry and/or government. The malicious code enables cyberespionage operations against the organizations whose systems are compromised.
- ▶ **Destructive Malware** — Sophisticated malware targets and destroys important data or prevents the system from booting successfully, rendering it unusable.
- ▶ **Ransomware** — Profit-seeking criminals target information systems with crucial data, such as computers used by governments, businesses, and even hospitals.
- ▶ **Advanced Persistent Threat (APT): Industrial Systems** — A nation state or well-financed, highly sophisticated actor develops malware that targets industrial control systems.
- ▶ **Cloud Provider Compromise** — A cyber-attack against a major cloud services provider, possibly a supply chain attack, gives malicious actors the ability to target the provider's clients, which may include industry and government, causing significant economic damage or compromising national security.



## DDoS Botnet Attack

**Malware infects a large number of devices to create a massive botnet and launch DDoS attacks against high value targets. The botnet may span dozens of countries and require significant international coordination to mitigate.**

### *Mirai Botnet*

On October 21, 2016, the Mirai Botnet targeted Dyn, a major DNS provider, with a wave of large distributed denial of service (DDoS) attacks.<sup>37</sup> A second attack struck two hours later, and this time customers could not access the websites of Dyn's customers such as Twitter, Netflix, Reddit, CNN, PayPal, and Spotify.<sup>38</sup> The botnet used to coordinate this attack was comprised of thousands of vulnerable devices such as CCTV cameras, which together fired 1.2 terabytes of data on Dyn, shutting down several large websites.<sup>39</sup> The scale and severity of the Mirai Botnet attack demonstrated the vulnerabilities within the global digital ecosystem and the growing threat that DDoS attacks pose to our businesses and organizations.

### *Evolution of IoT Botnets*

Since 2016, new attack vectors and delivery methods have been found that make botnets an even more serious hazard. For example, in January 2018, three large DDoS attacks were launched at several financial institutions, all built off the Mirai Botnet's source code.<sup>40</sup> Since then, the Mirai botnet's code has been publicly released.<sup>41</sup> So now criminals in different parts of the world can experiment and create their own variants of IoT botnets. Strategies that would have worked against Mirai will not necessarily work against newer botnets.<sup>42</sup>

For example, Mirai needed default passwords to gain control of devices. Newer botnets like Satori — which generated about 280,000 bots within 12 hours — Wicked, and Reaper have found ways around this weakness.<sup>43</sup> Because of the evolution of IoT botnets, many devices that would have been impervious to Mirai may end up becoming part of a botnet today.

To make matters worse, some of the new botnets can be rented for a low fee by cyber-criminals who lack the technical skills to make a botnet of their own. This arrangement, called malware-as-a-service (MaaS), expands the threat landscape to a broader set of bad actors.<sup>44</sup>

In early 2019, a Liberian telecom company became the subject of a lawsuit after hiring a criminal hacker to launch DDoS attacks against a rival to gain an unfair competitive advantage.<sup>45</sup> The hacker used a custom botnet based on Mirai and rented infected security cameras and routers from other hackers.<sup>46</sup> At their peak, the attacks disabled access for *most internet users in the country*, further adding to global concerns about IoT security.<sup>47</sup>

### DDoS Server-based Attack

**An attacker exploits the vulnerabilities in memcached servers to launch hugely amplified DDoS attacks. Because memcached servers — often used in cloud computing and Linux operating systems — do not require authentication, an attacker can falsify (“spoof”) the IP address of the computer contacting the servers. Most of the memcached servers belong to business enterprises and other organizations for which security is not a primary concern. By tricking a handful of servers into targeting a single fake address, an attacker can amplify the power of an attack thousands of times. Memcached server-based attacks currently hold the world record for largest DDoS attacks.**

#### *Vulnerable Memcached Servers*

On the first of March, 2018, the cloud service provider Akamai revealed that its client, GitHub, had been targeted by a DDoS attack measuring in at 1.3 Tbps.<sup>48</sup> This was the largest publicly recorded DDoS attack at the time.<sup>49</sup> The attack exploited a vulnerability in memcached servers — which are found mostly in cloud environments and communicate using protocols that operate without authentication, allowing pretty much anyone to request data from them.<sup>50</sup> According to Cloudflare, memcached servers respond with packets up to 51,000 times larger than the packets they receive. This allows attackers to coordinate much larger attacks using very little effort.<sup>51</sup>

Akamai was able to defend GitHub successfully using a number of mitigations strategies.<sup>52</sup> A few days later, however, an even bigger 1.7 Tbps DDoS attack targeted another service provider.<sup>53</sup> Such developments demonstrate how innovations in attack methods are being used to amplify DDoS attacks, testing the limits of providers’ capabilities.

In January 2019, a memcached attack was discovered to exceed 500 million packets per second (mpps), which is approximately four times the volume of the previous year’s attack on GitHub.<sup>54</sup> Since then, similarly high-volume attacks have been seen. While these attacks are not as large in terms of bandwidth as the record-setting 2018 attacks, the increase in attack volume is troubling because the sheer number of packets can exhaust network resources and can do as much damage as larger attacks.<sup>55</sup> A barrage of small attacks can also be used to mask deeper, more serious intrusions by avoiding detection while attackers gain foothold within compromised systems.<sup>56</sup>

### Border Gateway Protocol (BGP) Hijacking

**A BGP hijacking attack wrongfully redirects internet traffic and may cause disruptions to websites and online services while also enabling attackers to steal data, conduct espionage, and perpetrate other abuses. Sometimes, however, wrongful re-routing of IP addresses is a consequence of human error. Investigators may find it challenging to determine whether the hijacking was intentional and whether sensitive information was compromised.**

As a technique in the arsenal of bad actors, BGP hijacking has been used to target finance websites (e.g., Master Card, Visa) and cryptocurrency websites, among many other kinds of sites. Even more troublingly, in the hands of nation-states with adversarial goals, BGP hijacking may be perceived as a precursor to cyberwarfare and undermine confidence in the security of the interoperable internet ecosystem.<sup>58</sup>

### ***China Absorbs 15% of World's Internet Traffic in 2010***

In 2010, bad instructions issued by Chinese telecom companies routed traffic from multiple countries through Chinese servers — absorbing 15% of the global internet's traffic.<sup>59</sup> While the whole incident lasted less than 20 minutes, governments throughout the world took notice — in no small part because many websites with .gov and .mil domains were disrupted, including those belonging to the U.S. Senate and various branches of the military.<sup>60</sup> Some of the world's leading technology companies were also affected.<sup>61</sup>

The US-China Economic and Security Review Commission stated that “the Commission has no way to determine what, if anything, Chinese telecommunications firms did to the hijacked data” and “incidents of this nature could have a number of serious implications.”<sup>62</sup>

### ***2017 Russian Telecom Incidents***

In April 2017, a Russian controlled telecom seized control of traffic from two dozen financial services companies, including Visa and MasterCard.<sup>63</sup> Security experts noted that the incident was suspicious because normally accidental leaks absorb more traffic and are not limited to specific industries.<sup>64</sup> A few months later, in December 2017, major technology companies including Google, Facebook, Apple, and Microsoft discovered their traffic was being routed to a previously unheard of Russian internet service provider, again raising strong suspicions among the security community.<sup>65</sup>

### ***2018 Google Incident***

In November 2018, Google was revealed as the victim of a major BGP hijack — the worst in the company's history — targeting a broad array of services. Initial reports suggested that the attack, which has been traced to servers in Russia, China, and Nigeria (including servers of state-owned telecom companies) amounted to a “wargame experiment” and may be a prelude to even more severe attacks in the future.<sup>66</sup> Subsequent reports have pushed back against this account, explaining that the incident was caused by an erroneous BGP configuration of an ISP in Nigeria.<sup>67</sup> But as an article in *Forbes* points out, “If China isn't hijacking Internet traffic, there's no reason why not.”<sup>68</sup> The fact is that our current systems were built on trust and are exploitable by bad actors.

## **Domain Name System (DNS) Hijacking**

**Malicious actors alter information on a DNS server to redirect internet traffic to the wrong online destination, such as a fraudulent website that misleads the public. A fraudulent website may convincingly impersonate a well-known financial institution, government agency, or social media platform to deceive users into disclosing sensitive information (social security numbers, credit card numbers, passwords, etc.) It may also install various types of malware on user devices. Typically, if users know they correctly typed the URL of a legitimate website, they will not question its authenticity.**

One of the dangers of DNS hijacking is that misinformation can spread rapidly from one DNS server to another, creating an international incident.<sup>69</sup> Accidents involving DNS root server instructions have shown us what such a scenario looks like,<sup>70</sup> and more recent events prove the validity of longstanding concerns about exploitation of DNS vulnerabilities for cyber-espionage.<sup>71</sup>

### ***2010 Chinese DNS Root Server Incident***

In 2010, a Chilean ISP mistook DNS instructions from a root server in China — where certain websites cannot be accessed as a matter of national policy — with instructions meant for other parts of the world.<sup>72</sup> Neighboring ISPs trusted and shared the information provided by their peer.<sup>73</sup> Before long, the error spread all way to the United States. The consequences of this mistake became apparent to American users as they suddenly lost access to popular websites that are banned in China such as YouTube, Twitter, and Facebook.<sup>74</sup>

What is noteworthy about this incident from a security perspective is *how* the wrong DNS information spread. China purposely alters the instructions on its own root servers.<sup>75</sup> If a user in China types the URL of a prohibited website into a browser, they will not be able to access the destination associated with that URL because the DNS configuration takes them elsewhere: a government-controlled server.<sup>76</sup>

What this accident shows, therefore, is that users across the world can find themselves redirected to servers of a government that does not abide by international norms and exploits DNS vulnerabilities to conduct cyber-espionage, and the users may not even notice.<sup>77</sup>

### ***2019 DNS Hijacking Campaign***

In January 2019, FireEye reported that hackers with apparent ties to the Iranian government have engaged in massive DNS hijacking on a global scale to divert sensitive information from proper destinations into the custody of malicious actors.<sup>78</sup>

Stolen sensitive information included login credentials and non-public data from a variety of stakeholders in the global ICT ecosystem, including ISPs, government entities, and organizations in various continents: North America as well as North Africa, Europe, and the Middle East.<sup>79</sup>

The specific targets and category of data stolen match the Iranian governments' strategic interests.<sup>80</sup> Now that the bad actors have this data, they will be able to launch continuous cyber-attacks for years to come.<sup>81</sup> Security experts warn that this was just the first step in a bigger plan.

### **Software Vulnerabilities: Open Source**

**Malicious actors discover security vulnerabilities in open source software components, which are used in commercial applications that proliferate widely throughout the internet ecosystem. Open source vulnerabilities are a key point of discussion in supply chain risk management.**

Any discussion about open source vulnerabilities must start with the acknowledgement that there are many advantages to open source software, as evidenced by the degree of proliferation.<sup>82</sup> More than 95% of commercial applications today use some open source components and, on average, the open source components make up a third of the application's code.<sup>83</sup> The question is: In the absence of a specific developer to whom a software component can be directly attributed, how should the ICT stakeholder community work together to mitigate open source vulnerabilities?

### ***Equifax Data Breach and Follow-up***

In mid-May 2017, hackers exploited vulnerable open source code in Equifax web applications to steal social security numbers and other private information of 148 million people.<sup>84</sup> The code was known to be vulnerable for several months at the time when the breach occurred — yet the credit agency, like many other companies, did not act quickly enough to prevent data theft.<sup>85</sup>

The bigger ecosystem-wide problem is that Equifax is not alone. Currently, thousands of organizations download and use software known to be vulnerable, including the unpatched software that resulted in the theft of 148 million people's data.<sup>86</sup> In fact, only about one in five companies making use of the software have taken corrective measures after the breach.<sup>87</sup>

There are reasons for this: In the current state of the ecosystem, rapidly patching open source software components remains a challenge for many companies.<sup>88</sup> Part of the problem is that open source patches are sometimes difficult to update and a variety of technical difficulties prevent companies from being able to do so regularly.<sup>89</sup>

However, efforts are already underway within the ICT stakeholder community to collectively address this problem through market-based solutions and transparency measures.<sup>90</sup> These measures are being discussed in a variety of multi-stakeholder and partnership venues.<sup>91</sup>

### **Software Vulnerabilities: Zero Day**

**Malicious actors discover software zero day security vulnerabilities — vulnerabilities that software developers do not know about — and write exploit codes to gain unauthorized control and impair the functions of information systems all over the world. These can include corporate or government information systems containing highly sensitive information.**

The goal here is not to shame any particular company, but rather to identify ways that ICT companies can work together to spread information about security vulnerabilities when they affect the whole ecosystem and facilitate ecosystem-wide solutions. No matter how much a company invests in top coding talent and follows secure-by-design best practices, human mistakes in code will inevitably arise from time to time.

### ***Examples of Zero Day Vulnerabilities***

Bad actors often fall back onto zero-day exploits to execute their malicious codes. The exploits may be found in common products that millions of people use. For example, the exploit called CVE-2017-0199 abuses a logic flaw in Microsoft Word and fetches a remote resource from the internet — a malicious payload that attackers host online.<sup>92</sup> A substantially similar exploit is CVE-2018-9174, which leverages the library used by Internet Explorer to render web pages and ultimately download a payload on the victim's computer.<sup>93</sup> Even though Microsoft devotes significant resources to patching vulnerabilities, many of these threats can remain dangerous if businesses or individuals fall behind on updating their software.<sup>94</sup> Therefore, end-user awareness can be the difference between successfully securing the ecosystem against an exploit.



Zero day vulnerabilities are not merely an inconvenience to consumers — they can give rise to grave national security concerns. For example, it appears that in 2018 the Sejong Institute, a South Korean think tank that conducts national security research and holds large amounts of strategically important data, was attacked by hackers ostensibly from North Korea.<sup>95</sup> They accomplished this attack by exploiting a zero day vulnerability in Active X software.<sup>96</sup>

### ***Zero Day Vulnerability Disclosure***

Government agencies in charge of cybersecurity, for example the United States' NSA, have two often-irreconcilable interests when it comes to zero day vulnerabilities. They want to protect their own country and allies from preventable cyber-attacks.<sup>97</sup> On the other hand, by keeping zero day vulnerabilities secret, they gain a valuable instrument for disrupting opponents.<sup>98</sup> Because of these irreconcilable incentives, the government may or may not disclose security vulnerabilities.<sup>99</sup> The decision will be made situationally.

In general, global ICT leaders will patch vulnerabilities when they are discovered to be affecting consumers, provided the software is still supported. However, not all companies are subject to the same market forces or other external pressures. Some companies may be influenced by relationships with governments or other third parties. As global ICT leaders address the issue of zero day vulnerabilities, it is necessary to be open-eyed to the reality that not all players will always be motivated to maximize pre-incident protective capabilities through disclosure.

### **Hardware Vulnerabilities: Processor Architectures**

**A processor manufacturer identifies and discloses a vulnerability to a restricted set of ecosystem partners whose involvement in the coordination efforts is necessary for the vulnerability mitigation development and validation efforts. The manufacturer identifies mitigations, delivered through patches to microcode/firmware, operating system, and other system software, as needed. Validation, distribution, and installation of the mitigation often requires a multi-party coordinated vulnerability disclosure process, coordinated by the processor manufacturer.**

### ***Spectre and Meltdown***

The hardware vulnerabilities Spectre and Meltdown, disclosed in January 2018, took advantage of a feature called speculative execution common to most modern processor architectures.<sup>100</sup> The Spectre and Meltdown Proofs of Concept demonstrated the possibility of malicious actors using specific, targeted malware to infer data values that would normally be protected without proper authorization (for example sensitive data such as passwords). Thus, the great task of developing, testing, and deploying mitigations for these vulnerabilities in multi-party CVD settings has been a priority for industry.

Currently, there are no known instances of these vulnerabilities being exploited, and taking advantage of the vulnerabilities is difficult — a process that would require significant skill, planning, and investment.<sup>101</sup>

Spectre and Meltdown do, however, serve to illustrate some of the complexities inherent in responding to hardware vulnerabilities and distinct from most software vulnerabilities: (1) the number of parties that must coordinate is often greater in the hardware context, making coordination more difficult, and often more time-consuming due to that complexity;<sup>102</sup> (2) mitigations may involve multiple layers of the affected systems, not just

the hardware layer — a number of companies have released software patches that work around the problems caused by Spectre and Meltdown, including patches to microcode, firmware, operating systems, or other software (this requires coordination between and among multiple parties, led principally by the hardware vendor);<sup>103</sup> (3) distributing mitigations may involve parties other than the vendors themselves to develop, test and deliver the mitigations to end users, keeping information concerning these vulnerabilities in confidence while doing so.<sup>104</sup>

Notwithstanding these substantial challenges, there has been unprecedented coordination across ICT segments to address these kinds of vulnerabilities, and as processes continue to be refined mitigation efforts will benefit accordingly.

### Injection of Malicious Code in Software and Hardware Components

**A state-sponsored bad actor manages to insert malicious code into the software or hardware of major ICT companies, compromising systems in industry and/or government. The malicious code enables cyberespionage operations against the organizations whose systems are compromised.**

#### *Component Backdoors*

In recent years, policymakers have focused on the possibility of specific nation-states and bad actors inserting backdoors into ICT components manufactured overseas.<sup>105</sup> This is a complex issue as it may involve matters of supply chains, international trade, and economics — a full discussion of the policy implications is beyond the scope of this report.

In the past decade, even the NSA, an agency that protects critical U.S. security interests, may have faced serious challenges related to component backdoors.<sup>106</sup> This problem may have the potential to afflict industry as well.<sup>107</sup> For example, while the allegations of a 2018 *Bloomberg* report that China has inserted hardware backdoors into the supply chains of American companies have been strongly denied or met with strong skepticism by many segments of industry — including the companies whose supply chains would have been theoretically compromised — many experts in government, industry, and civil society nonetheless worry that such a feat is not technologically infeasible.<sup>108</sup> As such, the CSDE should discuss how the risk of injection of malicious code fits into its potentially broader engagement with issues of supply chain risk management.

### Destructive Malware

**Sophisticated malware targets and destroys important data or prevents the system from booting successfully, rendering it unusable. This malware can spread through the typical channels by which malware spreads. Once it infects a system, the malware's execution can be triggered remotely by an attacker's command or the malware can activate automatically after a defined amount of time.**

Malware with destructive capabilities comes in many forms and may have other features besides wiping data or rendering system assets unusable. For example, nation states have combined destructive malware with ransomware to obfuscate their motives, and Advanced Persistent Threat (APT) groups have covered their tracks by destroying digital evidence.<sup>109</sup>

One of the major challenges associated with destructive malware is the speed of execution. Often, by the time somebody discovers the malware's presence, it is already too late to defend the system or its data.<sup>110</sup> Because destructive malware can typically target the backup data on an infected system, storing backup data elsewhere is essential to recovery efforts.<sup>111</sup> The degree of destructive capability and the amount of data destroyed will vary depending on the specific techniques used to damage files or systems.<sup>112</sup>

### ***Shamoon***

Shamoon malware emerged in 2012 when politically motivated hackers targeted oil and gas companies in the Middle East.<sup>113</sup> The most notable target was Saudi Aramco — Shamoon disabled 30,000 of the company's workstations for nearly a month.<sup>114</sup> As a result of this cyber-attack, Saudi Aramco's ability to supply 10% of the global oil supply was put at risk.<sup>115</sup>

In 2016, Shamoon re-emerged and targeted petrochemical companies, as well as the Saudi central bank system.<sup>116</sup> This second version of the malware was considered a threat to mission-critical computers of targeted organizations.<sup>117</sup>

The latest version of Shamoon, which emerged in 2018, is even more destructive than its predecessors.<sup>118</sup> This is because it comes paired with a second piece of malware called Trojan.Filerase, which overwrites files on a computer while Shamoon itself targets the Master Boot Record (MBR), the part of a hard disk that provides information necessary to load the operating system.<sup>119</sup>

### ***BlackEnergy and GreyEnergy***

In December 2015, in the middle of winter, about 230,000 people in Ukraine lost power for six hours after a devastating cyber-attack on electricity distribution companies; the destructive malware used by the attackers is known as BlackEnergy.<sup>120</sup> This was the first widely recorded successful cyber-attack on an electrical grid, and experts worry it could be applied to many other critical systems, including hospitals.<sup>121</sup>

In October 2018, researchers at ESET released a whitepaper on GreyEnergy, a successor to Black Energy that targets critical infrastructure networks in Central and Eastern Europe.<sup>122</sup> This newer destructive malware remains a clear and present danger in the ecosystem.

### ***Wiper Ransomware***

Destructive malware has often been associated with ransomware attacks, even though deleting ransomed data has generally fallen out of favor among profit-seeking criminals. As Symantec explains, "you cannot easily monetize a computer that has been destroyed."<sup>123</sup>

In 2017, malware called NotPetya — a highly sophisticated cyber-attack disguised as ransomware — wreaked havoc across Europe, Asia, and the Americas.<sup>124</sup> The malware was unleashed by a nation state for the purpose of damaging specific systems and wiping out records with military precision, ensuring that the data cannot be recovered.<sup>125</sup> Altogether, the destruction from NotPetya resulted in over \$10 billions of damage, making it the costliest cyber-attack in history.<sup>126</sup>

Later the same year, in Japan, an extensive hacking campaign that exploited leaked NSA technology targeted the systems of companies across multiple industries; the attackers deployed destructive malware called ONI to cover their tracks.<sup>127</sup> While not as costly as NotPetya, this incident and others like it show that wiper ransomware is a growing trend.<sup>128</sup>

By combining destructive malware with ransomware, nation states and other sophisticated actors can sometimes succeed at making their intentions impenetrable to expert analysts.<sup>129</sup>

### ***Olympic Destroyer***

The opening ceremony of the 2018 Winter Olympics was disrupted by destructive malware called Olympic Destroyer. The malware was deployed in a cyber-attack that affected attendance — people could not print out their reservations — and coverage of the ceremony — the malware disabled internet access and telecasts, rendered drones unusable, and shut down the official Pyeongchang 2018 website.<sup>130</sup> Cisco's Talos security division concluded that because the malware wiped “all available methods of recovery” its purpose was destructive in nature.<sup>131</sup>

### ***VPNFilter***

In May 2018, Cisco's Talos security division issued an alert about VPNFilter, stealthy and highly versatile malware that has infected about a half-million home and small business routers.<sup>132</sup> While this malware currently serves an espionage function, researchers have determined it has worrisome destructive capabilities.<sup>133</sup> Part of the VPNFilter code is shared in common with BlackEnergy, the malware that caused power outages in Ukraine by attacking electricity distribution companies.<sup>134</sup> Most of the routers infected with VPNFilter are in Ukraine, and experts warn the malware may cause disruptions to targeted infrastructure.<sup>135</sup>

## **Ransomware**

**Profit-seeking criminals target information systems with crucial data, such as computers used by governments, businesses, and even hospitals. The criminals use malware that encrypts files on the infected systems, denying legitimate users access. A message then appears demanding payment in exchange for restored access. The proliferation of ransomware has been facilitated by ransomware-as-a-service (RaaS), which is when cybercriminals make malicious code available to less tech-savvy bad actors in exchange for agreed-upon compensation.**

**NOTE: In some cases, bad actors may disguise destructive cyber-attacks as ransomware. In these cases, the data may be impossible to recover even if victims are willing to pay the ransom.**

### ***Atlanta/WannaCry/Ransomware-as-a-Service***

Ransomware first emerged in Eastern Europe nearly a decade ago, when criminals locked up computers with malicious code and demanded payment in return for their restoration.<sup>136</sup> Since then ransomware has become much more prevalent and complex. It is used by profit-seeking individual hackers and sophisticated criminal organizations alike — they often demand virtual payment in the form of cryptocurrencies such as bitcoin.<sup>137</sup> In 2016, cybersecurity experts estimated that criminals reaped over \$1 billion in ransom payments using this attack method.<sup>138</sup> Attackers usually target organizations where downtime is not an option, such as in hospitals or

financial institutions.<sup>139</sup>

In 2018, the City of Atlanta was targeted by a sustained attack that demanded \$51,000 in return for the restoration of their computer network systems.<sup>140</sup> During this attack Atlanta's police officers were forced to write reports by hand, the court was unable to validate warrants, and the city stopped taking employment applications.<sup>141</sup>

Another severe series of attacks were orchestrated by a North Korean linked hacker group called Lazarus.<sup>142</sup> They produced a malware called "WannaCry" which crippled systems around the world that used Windows XP.<sup>143</sup>

A frightening development in the world of ransomware has been "Ransomware-as-a-Service".<sup>144</sup> This allows criminals lacking sophisticated technical knowledge the ability to commit effective attacks with the help of pre-made toolkits found in marketplaces on the Dark Web.<sup>145</sup> This phenomenon has promoted the creation and spread of thousands of different types and strains of ransomware, making remediation and attribution very challenging for those trying to fight this malware.<sup>146</sup>

### ***NotPetya Ransomware Attacks***

The NotPetya "ransomware" was born of a massive cyber-attack against Ukrainian institutions in 2017, allegedly by the Russian military.<sup>147</sup> The attack came cleverly disguised as ransomware of the type used by criminals to make a profit, in order to conceal the attacker's motive: damage to specific systems.<sup>148</sup> In specific cases, rather than encrypting data to ransom for payment, NotPetya wiped out computers' deep-seated records, ensuring that recovery of data was impossible.<sup>149</sup> To make matters worse, NotPetya did not stay contained to a single country. Before long, it spread across Europe, Asia, and the Americas — causing more than \$10 billion damages globally.<sup>150</sup>

The NotPetya outbreak was possible because of supply chain vulnerabilities, thereby raising concerns in the global stakeholder community about the trustworthiness of particular companies and the relationships between companies and particular governments.<sup>151</sup>

### ***Geographic Restrictions on Ransomware***

Ransomware attacks have infected machines all over the world, including machines in the countries where the ransomware originated.<sup>152</sup> Some of the more sophisticated modern ransomware only targets specific countries, or rather it is programmed not to target machines in specific countries.<sup>153</sup>

The Anatova ransomware discovered in early 2019 is a perfect example.<sup>154</sup> This advanced malware will not attack machines based in Russia and other CIS countries, as well as Egypt, India, Iraq Morocco, and Syria.<sup>155</sup> Many of the victims have been based in the United States.<sup>156</sup>

### **Advanced Persistent Threat (APT): Industrial Systems**

**A nation state or well-financed, highly sophisticated actor develops malware that targets industrial control systems. The malware may spread via means that do not require an internet connection (e.g., USB ports). The malware may infect computers in many different countries, looking for a strategically important target. When the malware finds the target, it can disrupt normal operations and result in severe damage.**



### ***Saudi Petrochemical Plant***

In August 2017, a Saudi petrochemical company was the victim of a cyber-attack that could have been lethal.<sup>157</sup> Experts believe the purpose of the attack was not merely the incapacitation of industrial systems but rather to trigger an explosion that could result in loss of human life.<sup>158</sup> The only reason an explosion did not take place is because of a computer coding error on the attackers' behalf.<sup>159</sup> Experts worry that similar attacks could take place in the future, possibly using similar exploits.<sup>160</sup>

### ***Global Nature of the Threat***

The sophisticated bad actors behind Trisis malware, which was used in the 2017 attack on a Saudi petrochemical company, have expanded their operations globally.<sup>161</sup> FireEye's research links the hacking group to Russia, specifically a lab in Moscow.<sup>162</sup> Multiple U.S. companies are among the targets of this group's cyber-attacks.<sup>163</sup> U.S. officials have publicly confirmed that hackers attempted to breach industrial control systems of firms that operate on US soil — this would enable the hackers to cause life-threatening damage.<sup>164</sup>

Details about attempted breaches of industrial systems cannot always be made public — for example, the names of companies breached, the number of companies breached, technical details of the breaches, and severity of threats to critical infrastructure may be withheld. However, it is clear that the government wants companies operating in the United States and elsewhere to be on high alert against APTs.<sup>165</sup> A common tactic for hackers is to compromise IT systems that have relatively low security, in order to gain a tactical foothold, before launching attacks aimed at more secure systems.<sup>166</sup>

### ***APT10/Chinese Cyber-Espionage***

In December 2018, the U.S. government attributed attacks carried out by the cyber-espionage group commonly known as APT10 — also known as Red Apollo, Stone Panda, CVNX, Potassium, and MenuPass — to the Chinese Ministry of State Security (MSS).<sup>167</sup> Known to be active since at least 2009, the APT10 group has targeted information that would be useful to the Chinese state during trade negotiations, as well as other high value intelligence assets.<sup>168</sup>

In particular, APT10 has targeted commercial entities of strategic interest to China including, according to FireEye's profile, companies involved in construction, engineering, aerospace, telecom and government.<sup>169</sup> APT10 has been notably active in the United States, Europe, and Japan. Recent APT10 targets include global managed service providers, such as IBM and Hewlett Packard Enterprise, and possibly other targets we do not yet know about.<sup>170</sup>

### **Cloud Provider Compromise**

**A cyber-attack against a major cloud services provider, possibly a supply chain attack, gives malicious actors the ability to target the provider's clients, which may include industry and government, causing significant economic damage or compromising national security.**

The cloud has undeniable benefits for organizations all over the world, including businesses and governments. With increased reliance on cloud services comes the need to secure unique attack surfaces in the cloud environment, including providers' own systems — to protect their clients' sensitive information of interest to bad actors.

***Operation Cloud Hopper***

The hacking group APT10, whose actions the United States has attributed to the Chinese government, carried out an extensive cyber-espionage campaign that began in 2014 and was not discovered until 2017.<sup>171</sup> Known as Operation Cloud Hopper, the campaign targeted managed service providers to infect their client companies with malware.<sup>172</sup> APT10 conducted this malicious series of attacks across fifteen countries in different regions of the world, including the United States and key allies.<sup>173</sup> According to experts at multiple security research groups, the Chinese hackers' targeting of managed service providers demonstrates their espionage tactics have evolved and accentuates the importance of addressing supply chain risks.<sup>174</sup>

***Cloudborne***

On February 26, 2019, security experts at Eclipsium Inc. revealed information about a cloud-based vulnerability known as Cloudborne.<sup>175</sup> The vulnerability could theoretically enable hackers to exploit components found in server motherboards that major cloud providers use in data centers.<sup>176</sup> According to the security experts at Eclipsium Inc., hackers can implant malware into the server's firmware or create a backdoor to steal data from the provider's clients.<sup>177</sup>

***Possibility of Massive Economic Damages***

According to the Ponemon Institute's 2017 Cost of Data Breach Study, the average data breach costs about \$3.62 million.<sup>178</sup> While this damage can be an enormous setback for an individual company — and the aggregate costs of such breaches are significant for the global economy — the average data breach will not generally rise to the level of a national security concern, unless the data stolen was of a particular nature.<sup>179</sup> On the other hand, the damage of a cyber-attack against a major cloud service provider could become a matter of national or global concern due not only to the type of data stolen but also because of the financial impact.<sup>180</sup> An attack against a cloud service provider could cause tens of billions of dollars in damage, with the highest estimate around \$120 billion in damages<sup>181</sup> — \$110 billion more than the costliest cyber-attack that has actually taken place and about a fifth of one percent of global GDP.<sup>182</sup>

To put this in further perspective, the damage from Superstorm Sandy was about \$70 billion<sup>183</sup> and the damage from Hurricane Katrina was about \$105 billion.<sup>184</sup> Which means a cyber-attack against a cloud service provider could be far more damaging economically than some of the worst natural disasters — and the attack could be about *twelve times* as damaging as the costliest cyber-attack in history.<sup>185</sup> It is essential, therefore, that we are well-positioned to coordinate as stakeholders to reduce the effectiveness of bad actors and mitigate against these kinds of worst-case scenarios.

## 09 | Endnotes

- 1 See generally Appendix A.
- 2 See FIRST, PSIRT Services Framework (2018), available at [https://www.first.org/education/FIRST\\_PSIRT\\_Service\\_Framework\\_v1.0](https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0). See also international standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018).
- 3 Irving Wladawsky-Berger, *GDP Doesn't Work in a Digital Economy*, THE WALL STREET JOURNAL (Nov. 3, 2017), <https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy>
- 4 Paul Tentena, *Artificial Intelligence to Double Digital Economy to 23 Trillion by 2025*, EAST AFRICAN BUSINESS WEEK (May 30, 2018), <http://www.busiweek.com/artificial-intelligence-to-double-digital-economy-to-23-trillion-by-2025>.
- 5 Danny Palmer, *Cloud computing: Why a Major Cyber-Attack Could Be as Costly as a Hurricane*, ZDNET (Jan. 17, 2018), <https://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane>.
- 6 See generally Appendix A.
- 7 Adam Vincent, *BlackEnergy Malware: How Hackers May Tackle our Infrastructure*, INFOSECURITY (Feb. 7, 2018), <https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure>.
- 8 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.
- 9 Andy Greenberg, *The White House Blames Russia for NotPetya, the "Most Costly Cyber Attack in History"*, WIRED (Feb. 15, 2018), <https://www.wired.com/story/white-house-russia-notpetya-attribution>.
- 10 See, e.g., Patel, *BlackEnergy, Grid-Disrupting Malware, Has a Successor, Researchers Warn*, POWER (Oct. 18, 2018), <https://www.powermag.com/blackenergy-grid-disrupting-malware-has-a-successor-researchers-warn/?pagenum=1>.
- 11 See, e.g., Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.
- 12 Nat'l Sec. Telecomm. Advisory Comm., NSTAC Report to the President on Internet and Communications Mobilization 12 (Nov. 16, 2017) [hereinafter NSTAC Report], available at <https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf>.
- 13 Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee on Incident Response*, DEPT OF HOMELAND SEC. (June 2016), [https://www.dhs.gov/sites/default/files/publications/HSAC\\_Cybersecurity\\_IR\\_FINAL\\_Report.pdf](https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf).
- 14 See, e.g., ENISA, *Strategies for Incident Response and Cyber Crisis Cooperation* (Aug. 25, 2016), <https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation>.
- 15 TechTarget, Network Operations Center, <https://searchnetworking.techtarget.com/definition/network-operations-center> (last accessed May 14, 2019).
- 16 NIST, Cybersecurity Framework, <https://www.nist.gov/cyberframework> (last accessed May 14, 2019).
- 17 See FIRST, PSIRT Services Framework v.1.0 (2018), available at [https://www.first.org/education/FIRST\\_PSIRT\\_Service\\_Framework\\_v1.0](https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0).
- 18 cyberSeek, Cybersecurity Career Pathway, <https://www.cyberseek.org/pathway.html> (last accessed May 14, 2019).
- 19 *Id.*
- 20 See ITU, Cybersecurity Information Exchange Techniques, <https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybex.aspx> (last accessed June 9, 2018).
- 21 The ability of the private sector (e.g., ISACs) to aggregate and correlate like incidents is considered foundational to cyber awareness and the creation of a common operating framework." NSTAC Report, supra note 10.
- 22 See generally Better Business Bureau, State of Cybersecurity Among Small Businesses in North America (2017), available at [https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity\\_final-lowres.pdf](https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf).
- 23 ENISA., Information Sharing and Analysis Centers, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing> (last accessed June 9, 2018).
- 24 NSTAC Report, supra note 10, at 21.
- 25 *Id.*
- 26 *Id.*
- 27
- 28 See, e.g., Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on the Bluetooth BR/EDR Vulnerability (Aug. 13 2019), <https://www.icasi.org/br-edr-encryption-key-bluetooth-vulnerability/addressing-a-Bluetooth-protocol-vulnerability-CVE-2019-9506>.
- 29 See international standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018). See also ENISA, ENISA REPORT ON GOOD PRACTICE GUIDE ON VULNERABILITY DISCLOSURE: FROM CHALLENGES TO RECOMMENDATIONS (2016), at 9 ("The global nature of the internet requires a more transnational approach to the topic of vulnerability disclosure"), available at <https://www.enisa.europa.eu/publications/vulnerability-disclosure>.

- 30 *Id.* International standards on coordinated vulnerability disclosure and handling processes, ISO/IEC 30111 (2013) (in renewal stages, 2019) and ISO/IEC 29147 (2018). *See also* THE CENTER FOR CYBERSECURITY POLICY AND LAW, IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE (2019), <https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure> for a discussion on Multi-Party CVD in the context of hardware.
- 31 NIST, Cybersecurity Framework, RS.AN-5, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (last accessed June 29, 2019).
- 32 FIRST, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (2017), *available at* [https://www.first.org/education/FIRST\\_PSIRT\\_Service\\_Framework\\_v1.0](https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0).
- 33 THE CENTER FOR CYBERSECURITY POLICY AND LAW, IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE (2019) 3, <https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure>.
- 34 *See also* the discussion on this issue in DIGITAL EUROPE, JOINT INDUSTRY LETTER ON CYBERSECURITY VULNERABILITIES ADMINISTRATIVE REGULATION RESPONSE TO MIIT PUBLISHED DRAFT FOR COMMENTS (July 18, 2019), <https://www.digitaleurope.org/resources/joint-industry-letter-on-cybersecurity-vulnerabilities-administrative-regulation-response-to-miit-published-draft-for-comments/>.
- 34 *Id.*
- 35 NSTAC Report, *supra* note 10, at 21.at ES—3.
- 36 ENISA, EU Cyber Cooperation: The Digital Frontline (2012), *available at* <https://www.enisa.europa.eu/publications/eu-cyber-cooperation-the-digital-frontline>.
- 37 Ben Bours, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017), <https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet> (reporting that a botnet experts feared “might be the work of a nation-state practicing for an attack” was revealed as the handiwork of a 21-year-old college student and his friends).
- 38 Brad Chacos, *Major DDoS Attack on Dyn DNS Knocks Spotify, Twitter, Github, PayPal, and More Offline*, PC WORLD (Oct. 21, 2016), <https://www.pcworld.com/article/3133847/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html>; *See also* Nicky Woolf, *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say*, THE GUARDIAN (Oct. 26, 2016), <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.
- 39 Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CYBERSCOOP (Oct. 27, 2016), <https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web>.
- 40 Zack Whittaker, *A New Mirai-Style Botnet Is Targeting the Financial Sector*, ZDNET (April 5, 2018), <https://www.zdnet.com/article/new-mirai-style-botnet-targets-the-financial-sector>.
- 41 Brian Krebs, *Source Code for IoT Botnet ‘Mirai’ Released*, KREBS ON SECURITY (Oct. 1, 2016), <https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released>.
- 42 *See* SentinelOne, *Mirai Botnet Descendants Will Lead to Even Bigger Internet Outages*, CSO (Dec. 22, 2016) <https://www.csoonline.com/article/3153031/mirai-botnet-descendants-will-lead-to-even-bigger-internet-outages.html>
- 43 *See, e.g.*, Grace Johansson, *Satori Botnet Able to Launch Crippling Attacks at Any Time*, SC MAGAZINE UK (Dec. 8, 2017), <https://www.scmagazineuk.com/satori-botnet-able-launch-crippling-attacks-time/article/1473666>; *See also* John Leyden, *OMG, That’s Downright Wicked: Botnet Authors Twist Corpse of Mirai into New Threats*, THE REGISTER (June 1, 2018), [https://www.theregister.co.uk/2018/06/01/mirai\\_respun\\_in\\_new\\_botnets](https://www.theregister.co.uk/2018/06/01/mirai_respun_in_new_botnets).
- 44 Chris Bing, *You can Now Buy a Mirai-Powered Botnet on the Dark Web*, CYBERSCOOP (Oct. 27, 2016), <https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web>.
- 45 Catalin Cimpanu, *Liberian ISP Sues Rival for Hiring Hacker to Attack Its Network*, ZDNET (Jan. 14, 2019), <https://www.zdnet.com/article/liberian-isp-sues-rival-for-hiring-hacker-to-attack-its-network>.
- 46 *Id.*
- 47 *Id.*
- 48 Brian Krebs, *Powerful New DDoS Method Adds Extortion*, KREBS ON SECURITY (Mar. 2, 2018), <https://krebsonsecurity.com/tag/memcached-attack>.
- 49 *Id.*
- 50 *Id.*
- 51 Cloudflare, *Memcached DDoS Attack*, <https://www.cloudflare.com/learning/ddos/memcached-ddos-attack> (last accessed Mar. 29, 2019).
- 52 Lily Newman, *Github Survived the Biggest DDOS Attack Ever Recorded*, WIRED (Mar. 1, 2018) <https://www.wired.com/story/github-ddos-memcached>.
- 53 Iain Thomson, *World’s Biggest DDoS Attack Record Broken After Just Five Days*, THE REGISTER (Mar. 5, 2018), [https://www.theregister.co.uk/2018/03/05/worlds\\_biggest\\_ddos\\_attack\\_record\\_broken\\_after\\_just\\_five\\_days](https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days).
- 54 Kacy Zurkus, *Largest DDoS Attack Sent Over 500 Million Packets per Second*, INFOSECURITY MAGAZINE (Jan. 30, 2019), <https://www.infosecurity-magazine.com/news/largest-ddos-attack-sent-over-500>
- 55 *Id.*
- 56 *See* Stephanie Weagle, *Short, Low-volume DDoS Attacks Pose Greatest Security and Availability Threat to Businesses*, ITPROPORTAL (July 7, 2017), <https://www.itproportal.com/features/short-low-volume-ddos-attacks-pose-greatest-security-and-availability-threat-to-businesses>.
- 57 *See, e.g.*, Dan Goodin, *Russian-controlled Telecom Hijacks Financial Services’ Internet Traffic*, ARS TECHNICA (Apr. 27, 2017), <https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic>.

58 See, e.g., Ms. Smith, *Possible BGP Hijacking Takes Google Down*, CSO (Nov. 13, 2018), <https://www.csoonline.com/article/3320996/possible-bgp-hijacking-takes-google-down.html> (explaining why a BGP incident could be perceived as a “war-game experiment”).

59 Nate Anderson, *How China Swallowed 15% of ‘Net Traffic for 18 Minutes*, ARS TECHNICA (Nov. 17, 2010), <https://arstechnica.com/information-technology/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes>.

60 *Id.*

61 *Id.*

62 *Id.*

63 See, e.g., Dan Goodin, *Russian-controlled Telecom Hijacks Financial Services’ Internet Traffic*, ARS TECHNICA (Apr. 27, 2017), <https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic>.

64 *Id.*

65 Dan Goodin, *“Suspicious” event routes traffic for big-name sites through Russia*, ARS TECHNICA (Dec. 13, 2017), <https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic>.

66 Ms. Smith, *Possible BGP Hijacking Takes Google Down*, CSO (Nov. 13, 2018), <https://www.csoonline.com/article/3320996/possible-bgp-hijacking-takes-google-down.html>.

67 Jane Lanhee Lee and Paresh Dave, *Nigerian Firm Takes Blame for Routing Google Traffic Through China*, REUTERS (Nov. 13, 2018), <https://www.reuters.com/article/us-alphabet-disruption/nigerian-firm-takes-blame-for-routing-google-traffic-through-china-idUSKCN1NI2D9>.

68 Emma Woollacott, *If China Isn’t Hijacking Internet Traffic, There’s No Reason Why Not*, FORBES (Nov. 13, 2018), <https://www.forbes.com/sites/emmawoollacott/2018/11/13/if-china-isnt-hijacking-internet-traffic-theres-no-reason-why-not/#24152e8e5ed5>.

69 Veracode, *Cache Poisoning*, <https://www.veracode.com/security/cache-poisoning> (last accessed Apr. 2, 2019).

70 See, e.g., Robert McMillan, *China’s Great Firewall Spreads Overseas*, COMPUTERWORLD (Mar. 25, 2010), <https://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html>.

71 Muks Hirani et al., *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FIREEYE (Jan. 9, 2019), <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html>.

72 *Id.*

73 *Id.*

74 *Id.*

75 *Id.*

76 *Id.*

77 *Id.*

78 Muks Hirani et al., *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FIREEYE (Jan. 9, 2019), <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html>.

79 Lily Newman, *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, WIRED (Jan. 11, 2019), <https://www.wired.com/story/iran-dns-hijacking>.

80 *Id.*

81 *Id.*

82 See Maria Korolov, *Open Source Software Security Challenges Persist*, CSO (Oct. 4, 2018), <https://www.csoonline.com/article/3157377/open-source-software-security-challenges-persist.html> (citing a study where the average application had 147 different open source components).

83 *Id.*

84 Robert Hackett, *Thousands of Companies Are Still Downloading the Vulnerability That Wrecked Equifax*, FORTUNE (May 7, 2018), <http://fortune.com/2018/05/07/security-equifax-vulnerability-download>.

85 *Id.*

86 *Id.*

87 *Id.*

88 *Id.*

89 *Id.*

90 Veracode, *Open Source Vulnerabilities*, <https://www.veracode.com/security/open-source-vulnerabilities> (last accessed Apr. 2, 2019).

91 See, e.g., NTIA, *Software Component Transparency*, <https://www.ntia.doc.gov/SoftwareTransparency>.

92 Kelly Sheridan, *Microsoft Office: The Go-To Platform for Zero-Day Exploits*, DARK READING (June 21, 2019), <https://www.darkreading.com/cloud/microsoft-office-the-go-to-platform-for-zero-day-exploits/d/d-id/1332114>.

93 *Id.*

94 Catalin Cimpanu, *Microsoft Releases Security Update for New IE Zero-Day*, ZDNET (Dec. 19, 2018), <https://www.zdnet.com/article/microsoft-releases-security-update-for-new-ie-zero-day>.

95 Charlie Osborne, *Lazarus Group Used ActiveX Zero-Day Vulnerability to Attack South Korean Security Think Tank*, ZDNET (June 13, 2018), <https://www.zdnet.com/article/north-korea-linked-lazarus-group-attacked-south-korean-think-tank-through-activex-zero-day>.

96 *Id.*



- 97 James Doubek, *Government Outlines When It Will Disclose Or Exploit Software Vulnerabilities*, NPR (Nov. 17, 2017), <https://www.npr.org/sections/alltechconsidered/2017/11/17/564755961/government-outlines-when-it-will-disclose-or-exploit-software-vulnerabilities>.
- 98 *Id.*
- 99 *Id.*
- 100 Josh Fruhlinger, *Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk*, CSO (Jan. 15, 2018) <https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html>.
- 101 THE CENTER FOR CYBERSECURITY POLICY AND LAW, *IMPROVING HARDWARE COMPONENT VULNERABILITY DISCLOSURE* (2019) 3, <https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure>.
- 102 *Id.* at 5–6. *See also* Digital Europe, Joint industry letter on Cybersecurity Vulnerabilities Administrative Regulation Response to MIIT published draft for comments (July 19, 2019), <https://www.digitaleurope.org/resources/joint-industry-letter-on-cybersecurity-vulnerabilities-administrative-regulation-response-to-miit-published-draft-for-comments/>.
- 103 *Id.* at 3.
- 104 *Id.* at 5–6.
- 105 *See, e.g.*, CISA, *CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams*, DEP'T OF HOMELAND SEC. (Feb. 26, 2019), <https://www.dhs.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams>.
- 106 Tom Simonite, *NSA's Own Hardware Backdoors May Still Be a "Problem from Hell"*, MIT TECH. REVIEW (Oct. 8, 2013), <https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell>.
- 107 *See* Dan Goodin, *Major US Telecom was Infiltrated by Backdoored Supermicro Hardware*, *Bloomberg Says*, ARS TECHNICA (Oct. 9, 2018), <https://arstechnica.com/gadgets/2018/10/new-bloomberg-report-says-backdoored-supermicro-hardware-infiltrated-major-us-telecom>.
- 108 Charlie Osborne, *Apple, Amazon Deny Claims Chinese Spies Implanted Backdoor Chips in Company Hardware: Report*, ZD NET (Oct. 4, 2018), <https://www.zdnet.com/article/how-one-tiny-chinese-chip-was-used-to-infiltrate-apple-amazon-us-contractors-report>.
- 109 ICS-CERT, Dep't of Homeland Sec., *Destructive Malware 1* (2017), [https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive\\_Malware\\_White\\_Paper\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf).
- 110 *Id.*
- 111 *See* Tara Seals, *Secrets of the Wiper: Inside the World's Most Destructive Malware*, THREATPOST (May 10, 2018), <https://threatpost.com/secrets-of-the-wiper-inside-the-worlds-most-destructive-malware/131836> (discussing how destructive malware can target “files (data), the boot section of the operating system of machines, and backups of system and data”).
- 112 Telefónica, *How Wiper Malware Affects Middle East and South America* 3 (2017), <https://www.elevenpaths.com/wp-content/uploads/2018/07/informe-impacto-del-malware-de-tipo-wiper-en.pdf>.
- 113 Symantec Security Response, *Shamoon: Back from the Dead and Destructive as Ever*, SYMANTEC (Nov. 30, 2016), <https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever>; Alexandre Mundo et al., *Shamoon Returns to Wipe Systems in Middle East, Europe*, MCAFEE (Dec. 14, 2018), <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe>.
- 114 Tara Seals, *Shamoon Reappears, Poised for a New Wiper Attack*, THREATPOST (Dec. 13, 2018), <https://threatpost.com/shamoon-new-wiper-attack/139881>.
- 115 Jose Pagliery, *The Inside Story of the Biggest Hack in History*, CNN (Aug. 5, 2015) <https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html>.
- 116 *Id.*
- 117 Symantec Security Response, *Shamoon: Back from the Dead and Destructive as Ever*, SYMANTEC (Nov. 30, 2016), <https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever>.
- 118 Security Response Attack Investigation Team, *Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail*, SYMANETC (Dec. 14, 2018), <https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail>.
- 119 *Id.*
- 120 Adam Vincent, *BlackEnergy Malware: How Hackers May Tackle our Infrastructure*, INFOSECURITY (Feb. 7, 2018), <https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure>.
- 121 *Id.*
- 122 ESET, *Grey Energy: A Successor to Black Energy* (Oct. 17, 2018), [https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET\\_GreyEnergy.pdf](https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf); *See also* Sonal Patel, *BlackEnergy, Grid-Disrupting Malware, Has a Successor, Researchers Warn*, POWER (Oct. 18, 2018), <https://www.powermag.com/blackenergy-grid-disrupting-malware-has-a-successor-researchers-warn/?pagenum=1>.
- 123 Symantec Security Response, *Destructive Malware: An Ever-Evolving Threat*, MEDIUM (Mar. 23, 2017), <https://medium.com/threat-intel/destructive-malware-evolution-392d3f8ef9d2>.
- 124 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.
- 125 *Id.*
- 126 *Id.*
- 127 Danny Palmer, *This Destructive Wiper Ransomware Was Used to Hide a Stealthy Hacking Campaign*, ZDNET (Nov. 1, 2017), <https://www.zdnet.com/article/this-destructive-wiper-ransomware-was-used-to-hide-a-stealthy-hacking-campaign>.

- 128 Assaf Dahan, *Night of the Devil: Ransomware or Wiper*, CYBEREASON (Oct. 31, 2017), <https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan> (noting that “targeted attacks involving ransomware/wipers have been on the rise across the world in recent years”).
- 129 See, e.g., Lindsey O’Donnel, *Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities*, THREATPOST (Mar. 27, 2019), <https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181> (noting that at time of the article’s publication “there has been no attribution to the attack, adding into the mystery when it comes to the malware developers’ underlying goals.”).
- 130 Nicole Perlroth, *Cyberattack Caused Olympic Opening Ceremony Disruption*, N.Y. TIMES (Feb. 12, 2018), <https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html>.
- 131 Warren Mercer and Paul Rascagneres, *Olympic Destroyer Takes Aim At Winter Olympics*, CISCO (Feb. 12, 2018), <https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>.
- 132 Andy Greenberg, *Stealthy, Destructive Malware Destroys Half a Million Routers*, WIRED (May 23, 2018), <https://www.wired.com/story/vpnfilter-router-malware-outbreak>.
- 133 See CISA, Dept’ of Homeland Sec., *VPNFilter Destructive Malware* (May 23, 2018), <https://www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware> (classifying VPNFilter as destructive malware).
- 134 Andy Greenberg, *Stealthy, Destructive Malware Destroys Half a Million Routers*, WIRED (May 23, 2018), <https://www.wired.com/story/vpnfilter-router-malware-outbreak>.
- 135 *Id.*
- 136 Alan Blinder and Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder* (Mar. 27, 2018), N.Y. TIMES <https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html>.
- 137 Emerging Technology from the arXiv, *True Scale of Bitcoin Ransomware Extortion Revealed*, MIT TECH. REVIEW (Apr. 19, 2018), <https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed>.
- 138 Alan Blinder and Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder* (Mar. 27, 2018), N.Y. TIMES <https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html>.
- 139 *Id.*
- 140 *Id.*
- 141 *Id.*
- 142 Catalin Cimpanu, *How US Authorities Tracked Down the North Korean Hacker Behind WannaCry*, ZDNET (Sept. 6, 2018), <https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry>.
- 143 Alexander Smith et al., *Why ‘WannaCry’ Malware Caused Chaos for National Health Service in U.K.* (May 17, 2017), <https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126>.
- 144 Stu Sjouwerman, *The Rise of Ransomware-as-a-Service*, CSO (Dec. 12, 2016), <https://www.csoonline.com/article/3147815/the-rise-of-ransomware-as-a-service.html>.
- 145 SentinelOne, *Ransomware as a Service: Hacking Made Easy*, CSO (Jan. 31, 2017), <https://www.csoonline.com/article/3163526/ransomware-as-a-service-hacking-made-easy.html>.
- 146 See David Bisson, *The Top 10 Ransomware Strains of 2016*, TRIPWIRE (Dec. 18, 2016), <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016>.
- 147 Andy Greenberg, *The White House Blames Russia for NotPetya, the “Most Costly Cyber Attack in History”*, WIRED (Feb. 15, 2018), <https://www.wired.com/story/white-house-russia-notpetya-attribution>.
- 148 *Id.*
- 149 *Id.*
- 150 *Id.*
- 151 ENISA, *Supply Chain Attacks* (Aug. 29, 2017), <https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks>.
- 152 See, e.g., Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.
- 153 See Bradley Barth, *Fresh-faced Anatova Ransomware Created by ‘Skilled Developers,’ Researchers Warn*, SC MAGAZINE UK (Jan. 23, 2019), <https://www.scmagazineuk.com/satori-botnet-able-launch-crippling-attacks-time/article/1473666>.
- 154 *Id.*
- 155 *Id.*
- 156 *Id.*
- 157 Nicole Perlroth and Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. TIMES (Mar. 15, 2018), <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>.
- 158 *Id.*
- 159 *Id.*
- 160 *Id.*
- 161 Sean Lyngaas, *FireEye Links Russia-owned Lab to Group Behind Trisis*, CYBERSCOOP (Oct. 23, 2018), <https://www.cyberscoop.com/trisis-russia-fireeye>.
- 162 *Id.*
- 163 Chris Bing, *Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms*, CYBERSCOOP (May 24, 2018), <https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos>.
- 164 *Id.*

- 165 See, e.g., U.S. CERT, Dep't of Homeland Sec., *Advanced Persistent Threat Activity Exploiting Managed Service Providers* (Oct. 3, 2018), <https://www.us-cert.gov/ncas/alerts/TA18-276B>.
- 166 Chris Bing, *Trisis Masterminds have Expanded Operations to Target U.S. Industrial Firms*, CYBERSCOOP (May 24, 2018), <https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos>.
- 167 Stilgherrian, At Least Nine Global MSPs Hit in APT10 attacks: ACSC, ZDNET (Dec. 21, 2018), <https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc>.
- 168 *Id.*; See also Jai Vijayan, China-Based Threat Actor APT10 Ramps Up Cyber Espionage Activity, DARK READING (Apr. 6, 2017), <https://www.darkreading.com/attacks-breaches/china-based-threat-actor-apt10-ramps-up-cyber-espionage-activity/d/d-id/1328584>.
- 169 FireEye, APT10, <https://www.fireeye.com/current-threats/apt-groups.html#apt10> (last accessed Mar. 29, 2019); See also William Tsing, *The Advanced Persistent Threat files: APT10*, MALWAREBYTES (Jan. 16, 2019), <https://blog.malwarebytes.com/cybercrime/2019/01/advanced-persistent-threat-files-apt10>.
- 170 Stilgherrian, At Least Nine Global MSPs Hit in APT10 attacks: ACSC, ZDNET (Dec. 21, 2018), <https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc>.
- 171 Jai Vijayan, *APT10 Indictments Show Expansion of MSP Targeting, Cloud Hopper Campaign*, DARK READING (Dec. 21, 2018), <https://www.darkreading.com/threat-intelligence/apt10-indictments-show-expansion-of-msp-targeting-cloud-hopper-campaign/d/d-id/1333539>; See also PwC UK and Bae Systems, OPERATION CLOUD HOPPER (Apr. 2017), <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>.
- 172 *Id.*
- 173 Dark Reading Staff, *Chinese APT10 Hacking Group Suspected of Global Campaign Targeting MSPs*, DARK READING (Apr. 5, 2017), <https://www.darkreading.com/attacks-breaches/chinese-apt10-hacking-group-suspected-of-global-campaign-targeting-msps/d/d-id/1328563>.
- 174 Davis Bond, *Hackers Target Cloud Services*, FINANCIAL TIMES (July 12, 2018), <https://www.ft.com/content/4f990a78-537a-11e8-84f4-43d65af59d43> (discussing PwC's analysis of Operation Cloud Hopper in the context of supply chain risk); Jai Vijayan, *APT10 Indictments Show Expansion of MSP Targeting, Cloud Hopper Campaign*, DARK READING (Dec. 21, 2018), <https://www.darkreading.com/threat-intelligence/apt10-indictments-show-expansion-of-msp-targeting-cloud-hopper-campaign/d/d-id/1333539> (quoting FireEye's senior manager of cyber espionage as stating that APT10's "move towards compromising managed service providers (MSPs) showcases the danger of supply chain compromises and reflects their continuously evolving tactics").
- 175 Maria Deutscher, *New Cloudborne Vulnerability Exposes Cloud Servers to Potential Hacking*, SILICONANGLE (Feb. 26, 2019), <https://siliconangle.com/2019/02/26/new-cloudborne-vulnerability-potentially-exposes-cloud-servers-hacking>.
- 176 *Id.*
- 177 *Id.*
- 178 Ponemon Institute, 2017 COST OF DATA BREACH STUDY (June 2017), <https://www.ibm.com/downloads/cas/ZYKLN2E3>.
- 179 See Susan Landau, *Understanding Data Breaches as National Security Threats*, LAWFARE BLOG (Feb. 26, 2018), <https://www.lawfareblog.com/understanding-data-breaches-national-security-threats>.
- 180 Tim Worstall, *Lloyd's - Extreme Cyberattack Could Cost \$120 Billion, As Much As 0.2% Of Global GDP*, FORBES (July 17, 2017), <https://www.forbes.com/sites/timworstall/2017/07/17/lloyds-extreme-cyberattack-could-cost-120-billion-as-much-as-0-2-of-global-gdp/#20d26ed46cc3>.
- 181 *Id.*
- 182 Compare Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world> (discussing the \$10 billion damages caused by NotPetya) with Tim Worstall, *Lloyd's - Extreme Cyberattack Could Cost \$120 Billion, As Much As 0.2% Of Global GDP*, FORBES (July 17, 2017), <https://www.forbes.com/sites/timworstall/2017/07/17/lloyds-extreme-cyberattack-could-cost-120-billion-as-much-as-0-2-of-global-gdp/#20d26ed46cc3>.
- 183 CNN, *Hurricane Sandy Fast Facts*, <https://www.cnn.com/2013/07/13/world/americas/hurricane-sandy-fast-facts/index.html> (last accessed Apr. 2, 2019).
- 184 Danny Palmer, *Cloud computing: Why a Major Cyber-Attack Could Be as Costly as a Hurricane*, ZDNET (Jan. 17, 2018), <https://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane>.
- 185 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>.







# The C2 Consensus on IoT Device Security Baseline Capabilities

ALLIANCE FOR  
TELECOMMUNICATIONS  
INDUSTRY SOLUTIONS

ASSOCIATION OF HOME  
APPLIANCE MANUFACTURERS

BSA | THE SOFTWARE ALLIANCE

CABLELABS

COALITION FOR CYBERSECURITY  
POLICY AND LAW

COMPTIA

CONSUMER TECHNOLOGY  
ASSOCIATION

COUNCIL TO SECURE THE  
DIGITAL ECONOMY

CTIA

INDUSTRIAL INTERNET  
CONSORTIUM

INFORMATION TECHNOLOGY  
INDUSTRY COUNCIL

INTERNET OF SECURE THINGS

INTERNET SOCIETY

IOTOPIA

NCTA — THE INTERNET &  
TELEVISION ASSOCIATION

OPEN CONNECTIVITY  
FOUNDATION

TELECOMMUNICATIONS  
INDUSTRY ASSOCIATION

UL

U.S. CHAMBER OF COMMERCE

USTELECOM — THE BROADBAND  
ASSOCIATION



Council to Secure the  
Digital Economy

## Acknowledgement

The following organizations contributed technical material, provided ongoing advice and support, and helped craft the recommendations in this document. The editors gratefully acknowledge the contributions of these and other groups:

---

Alliance for Telecommunications Industry Solutions (ATIS)

---

Association of Home Appliance Manufacturers (AHAM)

---

BSA | The Software Alliance

---

CableLabs

---

Coalition for Cybersecurity Policy and Law

---

CompTIA

---

Consumer Technology Association (CTA)

---

Council to Secure the Digital Economy (CSDE)

---

CTIA

---

Industrial Internet Consortium (IIC)

---

Information Technology Industry Council (ITI)

---

Internet of Secure Things (IoXT)

---

Internet Society

---

IoTopia

---

NCTA — The Internet & Television Association

---

Open Connectivity Foundation (OCF)

---

Telecommunications Industry Association (TIA)

---

UL

---

U.S. Chamber of Commerce (USCC)

---

USTelecom - The Broadband Association (USTelecom)

---

## LETTER FROM

**Gary Shapiro, President and Chief Executive Officer, CTA**

**Jonathan Spalter, President and Chief Executive Officer, USTelecom**

---

ALONG WITH THE TREMENDOUS BENEFITS that the rapid growth of the Internet of Things (IoT) brings to consumers, businesses, governments and the global digital economy, the IoT's growth also brings increased threats to the digital economy.

This is why the Council to Secure the Digital Economy (CSDE) — composed of USTelecom, the Consumer Technology Association (CTA), and 13 global information and communications technology (ICT) companies — has convened technical experts from 19 leading organizations throughout the ICT sector to develop and advance industry consensus on baseline security capabilities for new devices.

This convening of the conveners — or C2 — has brought together trade associations, standards development organizations, industry alliances and coalitions to develop the C2 Consensus Baseline, the broadest and most technically deep industry consensus on IoT security worldwide. This effort is based on the principle that the best way to achieve IoT security is for technical experts to develop and advance security specifications that will spread throughout the global market.

This document provides clear expert guidance to industry and government on securing new IoT devices in order to raise the market's expectations for security and to advance global policy harmonization. It is our expectation that this global approach will prove more effective than disparate local initiatives that would fragment security requirements and cause inefficiencies in the market that result in weaker security.

We thank all C2 participants, which collectively represent thousands of companies and many different segments of the global digital economy, for their engagement and their valuable contributions.

We look forward to promoting the C2 Consensus Baseline in key venues around the world to move the global market for IoT toward security.

Sincerely,



Gary Shapiro  
*President and CEO, Consumer Technology Association*



Jonathan Spalter  
*President and CEO, USTelecom*





## Contents

<b>01</b>	Foreword .....	4
<b>02</b>	Definitions and Acronyms .....	5
<b>03</b>	Background .....	6
<b>04</b>	Methodology .....	9
<b>05</b>	Consensus Baseline IoT Device Security Capabilities .....	10
	5.1. <i>Secure Device Capabilities – Baseline</i> .....	10
	5.1.1. Device Identifiers .....	10
	5.1.2. Secured Access .....	12
	5.1.3. Data In Transit Is Protected .....	13
	5.1.4. Data At Rest Is Protected .....	14
	5.1.5. Industry Accepted Protocols are Used for Communications .....	15
	5.1.6. Data Validation .....	15
	5.1.7. Event Logging .....	16
	5.1.8. Cryptography .....	16
	5.1.9. Patchability .....	17
	5.1.10. Reprovisioning .....	18
	5.2. <i>Product Lifecycle Management Capabilities - Baseline</i> .....	18
	5.2.1. Vulnerability Submission and Handling Process .....	18
	5.2.2. EoL/EoS Updates and Disclosure .....	19
	5.2.3. Device Intent Documentation .....	19
<b>06</b>	Annex A: Regarding Future Secure Capabilities – Phase in Over Time .....	21
	A.1 <i>Device Intent Signaling</i> .....	21
	A.2 <i>Device Network Onboarding</i> .....	21
<b>07</b>	Annex B: Additional IoT Device Security Capabilities and Practices .....	23
	B.1. <i>Secure Development Lifecycle</i> .....	23
	B.2. <i>Hardware Rooted Security</i> .....	23
	B.3. <i>Time Distribution</i> .....	24
	B.4. <i>System Resiliency</i> .....	24
	B.5. <i>Secure Toolchains</i> .....	25
	B.6. <i>Software Transparency and Bill of Materials</i> .....	25
	B.7. <i>Least Functionality</i> .....	26
	B.8. <i>Physical Access Control</i> .....	26
	B.9. <i>Best Current Practices</i> .....	26



<b>08</b>	Annex C: Discussion of Implementation and Complexity .....	27
<b>09</b>	Annex D: Informative References .....	30
<b>10</b>	Annex E: Mapping to CSDE International Anti-Botnet Guide.....	31
<b>11</b>	Annex F: Mapping to CTIA IoT Device Cybersecurity Certification .....	34
<b>12</b>	Annex G: Mapping to IoTopia Specifications.....	37
<b>13</b>	Annex H: Mapping to IoXT Pledge .....	41
<b>14</b>	Annex I: Mapping to Open Connectivity Foundation Specifications .....	44
<b>15</b>	Annex J: Mapping to World Wide Web Coalition Web of Things Requirements.....	47
<b>16</b>	Annex K: Mapping to EU Agency for Cybersecurity Baseline Security Recommendations for IoT.....	49
<b>17</b>	Annex L: Mapping to ETSI 103 645 .....	54
<b>18</b>	Annex M: Mapping to GSMA IoT Security Guidelines for Endpoint Ecosystems.....	57
<b>19</b>	Annex N: Mapping to Draft NISTIR 8259.....	60
<b>20</b>	Annex O: Mapping to UK DCMS Code of Practice for Consumer IoT Security .....	63
<b>21</b>	Annex P: Mapping to UL MCV 1376 – Security Capabilities Verified .....	66
<b>22</b>	Sponsoring Organizations .....	75
<b>23</b>	Endnotes .....	76





## 01 | Foreword

**THE CONVENE THE CONVENERS (C2) PROJECT** coalesces the expertise of hundreds of technical experts via their various conveners: trade associations, standards development organizations, industry alliances and coalitions. The C2 Consensus was developed by many organizations working together on an equal basis to find common ground on IoT device security for new designs. The convening—bringing together—of these groups allowed for sharing and comparing the expert recommendations each had developed within their own constituency. The work was coordinated under the auspices of the Council to Secure the Digital Economy and the Consumer Technology Association.

This is a technical document. Beyond the general technical security principle that the best path to IoT security is for technical experts to develop and advance technical security specifications, any questions of law, regulation, and policy pertaining to data security and privacy are out of scope for this document. (Where the term “policy” is used, it is intended to reference technical and operational policies rather than, for instance, regulatory policies.)

Although the contributors to the C2 Consensus recognize that the security of the installed base of legacy devices is important, this document applies to new device designs.

It is important to note that “consensus” is not a synonym for “unanimity”. Where there was not perfect agreement among C2 participants, the key pros and cons of certain recommendations are captured here.

It is also important to recognize that this Consensus document does not replace or supersede the security work done by these organizations. Each technical document that was used to draft this Consensus document has its place in the IoT world and should be considered on its own merits and in its own context.

## 02 | Definitions and Acronyms

<b>Configuration</b>	The device data related to device identity, credentials and associated data that support that identity
<b>Credential</b>	Evidence that supports a claim of identity.*
<b>Cryptographic</b>	
<b>Certificate</b>	A cryptographically signed structure that binds public keys to an identifier for the entity (i.e., a distinguished name).
<b>Device</b>	An entity with one or more endpoints.
<b>Endpoint</b>	An entity comprised of one or more components, addressable on a network.
<b>Entity</b>	An item with a recognizably distinct existence.†
<b>EoL</b>	End of Life (of an IoT device)
<b>EoS</b>	End of Service (of an IoT device)
<b>Identity</b>	An inherent property of an entity that distinguishes it from all other entities; an identity must exist in a namespace to allow it to be referred to without ambiguity.‡
<b>IoT</b>	Internet of Things. An IoT system involves a physical device that connects to a switched or wireless network, for the purposes of access and control. IoT systems may be connected to open networks, such as the Internet, or closed private networks. An IoT device may have supplementary functions provided through remote execution such as an application running on a phone, tablet, local or 'cloud' based computing system.
<b>Managed</b>	(Of environments), supported by trained staff (beyond manufacturer technical support), such as in a large enterprise or in a government office. Compare with unmanaged environment.
<b>PKI</b>	Public Key Infrastructure
<b>Policy</b>	Policy refers to applicable laws, regulations, and corporate policy.
<b>Post-market</b>	After release of the individual device to the field (i.e., after it leaves the factory and goes into the distribution channel). Compare to pre-market.
<b>Pre-market</b>	Prior to release of the individual device to the market (e.g., before it leaves the factory and goes into the distribution channel). Compare to post-market.
<b>Root of Trust</b>	(Also RoT) A component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update.
<b>Unmanaged</b>	(Of environments), not supported by the owning organization's staff, such as a consumer home or some small businesses.

\* CNSSI 4009, available at <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>

† ISO/IEC 24760-1:2011, available at <https://www.iso.org/standard/57914.html>

‡ ISO/IEC/IEEE 31320-2:2012, available at <https://www.iso.org/standard/60614.html>



## 03 | Background

### IoT Growth and Security

**IT HAS BEEN WELL-DOCUMENTED** that the Internet of Things (IoT) is growing quickly; the rapid deployment of connected devices is estimated to reach 20 billion units by 2020.<sup>1</sup> This incredible growth is fueled by falling integration costs, explosion of use cases and ubiquitous connectivity.

IoT adoption brings new technologies to many verticals, including manufacturing, medical, automotive, and consumer. In many cases these new technologies may also offer greater robustness, safety, reliability, and resilience by allowing the device to have real-time updates to address security flaws, whereas prior to this technology, such updates were not possible. Still, these technologies often introduce new concerns regarding the safety, reliability, security, resilience, and privacy of the device, leading to potential reduction in the overall trustworthiness of the system. Security is the common denominator across these inter-related trustworthiness disciplines and the security assures they operate as intended. Securing the IoT is a multifaceted challenge that demands a layered approach: security must be addressed not only in IoT devices but also in the network infrastructure, cloud architectures, edge providers, and other elements of the IoT that interact with those devices. Nevertheless, the trustworthiness of the IoT begins with secure devices.

Therefore, while this document acknowledges the relevance and importance of the related trustworthiness disciplines, it focuses exclusively on the security aspects of IoT devices themselves.

The security challenges of the IoT are also well-publicized. Botnets have become particularly and increasingly damaging and costly; they propagate malware,<sup>2</sup> conduct denial of service attacks,<sup>3</sup> and spread disinformation on social media.<sup>4</sup> A single botnet can now include more than 30 million “zombie” endpoints and allow malicious actors to profit six figures per month.<sup>5</sup>

Aside from being compromised at scale to form botnets, poorly secured IoT devices can be compromised to send spam, secretly collect user data, and hijacked for malicious remote control. Due to the critical nature of many of these devices, as well as the potential to use them as launch points for more damaging attacks, the Center for Strategic & International Studies (CSIS) released a report emphasizing the need for the federal government to consider cybersecurity as a key pillar in its procurement and use of endpoint devices, inclusive of IoT.<sup>6</sup>

### Many Efforts, Many Standards

Industry is moving to lock down the IoT in a variety of ways. These methods include software and hardware wrappers to thwart device attacks, and modified traditional security appliances such as firewalls and IDPS specifically designed to focus on the IoT.<sup>7</sup>

While individual industry segments work on security, broad efforts are underway to address this challenge in a harmonized fashion. These efforts are occurring in all parts of the globe. Regulators and other government agencies in many parts of the world have established or are establishing recommendations and requirements, assessment structures and labeling programs.

- 
- ▶ **European Union:** The Cybersecurity Act<sup>8</sup> will, among other things, allow the EU Agency for Cybersecurity (formerly the EU Agency for Network and Information Security, or ENISA) to set certification schemes for ICT products, services, and processes, to include the IoT.
  - ▶ **Japan:** The Ministry of Economy, Trade and Industry (METI) is developing a Cyber/Physical Security Framework<sup>9</sup> pertaining to the security of IoT and other connected systems.
  - ▶ **Singapore:** The Infocomm Media Development Authority is developing an IoT Cyber Security Guide.
  - ▶ **United Kingdom:** The Department for Digital, Culture, Media and Sport is active on these issues, for instance issuing a Code of Practice for Consumer IoT Security<sup>10</sup> and recommending regulations to require consumer IoT devices incorporate at least minimum security controls.<sup>11</sup>
  - ▶ **United States:** The National Institute of Standards and Technology (NIST) has established the Cybersecurity for IoT Program.<sup>12</sup>

Civil society groups are working in similar directions<sup>13</sup>. And of course, industry organizations—trade associations, standards development organizations, industry alliances and coalitions—have crafted a variety of voluntary consensus standards and “best practice” documents for securing IoT devices.<sup>14</sup>

Some of these industry documents are best used in a specific context. They may be aimed at vertical markets such as the smart home or medical device markets; or have other contextual boundaries. Other documents are intended for horizontal market application. They are independent of specific application.

### The Need for a Common Baseline

Each industry group makes an important contribution in their space and in general, by convening technical experts to build well-thought-out and effective recommendations. But the multiplicity of expert recommendations does create questions about where to start, how to consider such a wealth of overlapping recommendations, and which ones to follow.

There is a need for a common baseline of security capabilities for all IoT devices. Recommendations and requirements for such capabilities that are in place and under development are fragmented. Bringing consensus and harmonization to the current fragmentation will increase the market’s ability to promote IoT security by creating efficiencies of scale in development, manufacturing, support, training, assessment and identification of IoT products with increased security controls.

### C2: Convening the Conveners

The C2 project is convening the leveraged expertise of hundreds of technical experts via their conveners: trade associations, standards development organizations, industry alliances and coalitions. The participants and contributors to the C2 process have worked to compare their own technical specifications to those of other such groups.

Each group represents anywhere from dozens to thousands of companies. A number of the groups are international in scope. The technical expertise in the Consensus is informed, therefore, by a global legion of

industry security professionals. The Consensus cannot capture the perspectives and capabilities of all parts of the IoT ecosystem, but it recognizes a few key baselines that can be commonly pursued and flexibly implemented by manufacturers and others that are looking for guidance.

The Consensus articulates the accepted commonalities in IoT device security and also identifies the areas where consensus has not yet developed. In the latter cases, this document notes why consensus is lacking, in what context it may be found, and in some cases offers suggestions about how to achieve complete consensus on such items.

### Application of the Consensus

The Consensus Baseline IoT Device Security Capabilities (the “baseline”) is a common set of device security capabilities that can be applied to all new IoT devices that connect to the internet. The baseline is a set of best-practice capabilities that are broadly applicable—vertically and horizontally—across markets. It applies to the diverse range of new IoT devices, accommodating the broad spectrum of device complexity, regardless of the deployment environment. The baseline is intended to be flexible and not prescriptive. Depending on a variety of factors—from device complexity, deployment environment (managed or unmanaged), risk profile, use case and context—the security capabilities outlined in the baseline can be achieved in a variety of ways, with the key being that the ultimate baseline capability is achieved in a way that is applicable to the specific device. For example, a connected dog collar has a different risk profile than a device that is part of an industrial IoT system; the dog collar is less complex and is likely not part of a managed deployment. Both devices should be secure and meet the common set of security capabilities set forth in the baseline, but *how* to meet each capability will vary, just as the risk profile of IoT devices varies.

Likewise, the baseline is a starting point for IoT device security that will need to evolve over time based on both changes in technology and changes to the threat landscape. This document is intended to inform further work on capabilities for IoT device cybersecurity that is more targeted to specific verticals, device types, use cases, etc.

The baseline is also intended to contribute towards government IoT security efforts. For example, the United States Department of Commerce NIST Cybersecurity for IoT Program is in a public process of developing IoT device baseline capabilities that are informed, in part, by NISTIR 8228, *Considerations for Managing IoT Cybersecurity and Privacy Risk*,<sup>15</sup> and Draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*.<sup>16</sup> C2 participants expect that this Consensus will contribute to that process. More broadly, the global nature of the participants in C2 means that the Consensus should be interesting and important in many jurisdictions, industries, and vertical markets.

The purpose and benefits of this Consensus are two-fold and mutually reinforcing. First and most important, advancing toward an industry consensus security baseline will promote IoT security throughout the global market. The baseline will help to lift *all* new IoT devices’ cybersecurity; the fact that most of the IoT market is comprised of low- or medium-complexity devices<sup>17</sup> makes it all the more important for the baseline to be applicable to low- and medium-complexity devices, and not tailored for high-complexity devices. Second, consensus in industry will streamline and strengthen government-industry collaboration on these issues, allowing for more effective IoT security policies worldwide — and thus bring further improvements in IoT security.





## 04 | Methodology

**CSDE BEGAN THIS PROCESS** by surveying the IoT device security capabilities recommendations and voluntary consensus standards available. Those groups that had already contributed important work were identified in a linear list. The list included groups from industry, government and civil society. This initial enumeration amounted to dozens of organizations, too many for a realistic process of consensus-building.

In order to manage the effort, the C2 project team identified a subset of these organizations as potential sources of technical recommendations for a consensus process. Most are from industry. Government and civil society groups have technical expertise as well, of course, but the industry groups leverage the in-house subject matter experts as well as the pragmatic capabilities of the engineers who are building products. Further, government recommendations often follow a public consultation model, bringing in the same industry experts to comment on proposals.

Once the C2 organizations were assembled, each was asked to submit proposed IoT device security capabilities in a standardized format.

The group met March 21st 2019 to compare the data and identify common capabilities. thirteen consensus capabilities were identified. These are identified and explained in Section 5, *“Consensus Baseline IoT Device Security Capabilities”*. As guidance for the future, selected capabilities that are important but still emerging are shown in *“Annex A: Regarding Future Secure Capabilities — Phase In Over Time”*. Those requirements that did not, in the opinion of the group, achieve consensus status are listed in *“Annex B: Additional IoT Device Security Capabilities”*.

“Consensus” in this process did not always represent unanimity but always required a significant majority. Where there was not unanimity, the counterpoints are included in Section 5, *Consensus Baseline IoT Device Security Capabilities*, along with the majority points.

Finally, this is a technical document. Discussions of law, regulation and future law and regulation on data security and privacy are out of scope for this document. Where the term “policy” is used, it is used to clarify application of technical topics. Generally, “policy” here will refer to applicable law, applicable regulation, and corporate decisions (“corporate policy”) about the handling of material. Cybersecurity, as an engineering practice, protects the confidentiality, integrity and availability of that which policy determines is to be protected.



## 05 | Consensus Baseline IoT Device Security Capabilities

**THIS SECTION IDENTIFIES** specific “core” baseline security capabilities applicable to all IoT devices.

The first subsection of the baseline, Section 5.1 identifies *device capabilities*. Device capabilities are tangible, testable and verifiable mechanisms built into IoT devices. Broader organizational capabilities for a secure lifecycle are identified in Section 5.2. A third category, secure development, and more generally, organizational cybersecurity risk management practices are beyond the scope of this document.

Some items were identified as important but there was not consensus that the enabling technology was well-enough adopted or developed. Because these items were deemed significant over time, they are included in Annex A as “phase in over time” topics, and should be reviewed by developers for possible future inclusion.

### 5.1 SECURE DEVICE CAPABILITIES — BASELINE

This section includes device capabilities that are properties of the hardware and software, as opposed to business or development processes or capabilities.

#### 5.1.1 Device Identifiers

---

**Definition:** A unique value associated with the endpoint (or values associated with the functional entities within the endpoint) that exists in a namespace to allow it to be referenced without ambiguity. This value is distinct and distinguishes a device from all other devices.

---

**Scope:** Identity in the context of device authentication, authorization and management

---

**Discussion:** The goal of this capability is to utilize identify information to identify and differentiate a device on the network.

Identity is represented by a single or multiple identifiers. Identifiers play a critical role for IoT security. They are used to address functions and attributes of an IoT device as unique instances which can then be accessed, operated and managed. Identifiers are not just hardware based but can be used for applications and other IoT entities.

Identities play a role across the entire device lifecycle. Identifiers are used to onboard devices to a network(s), register, authenticate, authorize, assign access lists and policy, control and manage the device in the performance of services and applications. Identifiers are used to enumerate the network and identify devices that are or are not intended to be on the network and help trace issues in the event of a breach. Identifiers must be unique, stored and protected. Note that a single device may have multiple entities within the device. These entities could be sub-systems, applications and or services.



It should be noted that the security benefit of these identifiers can be bolstered by additional cryptographic protections for confidentiality, integrity and availability.

For low-end devices, a simpler identifier may suffice to achieve this capability. For example, some resource constrained devices may not be able to mutually authenticate with another device, sign/verify a digital signature, etc. In these cases, the device should be designed to implement as much security as is feasible. In some cases, this may simply consist of not storing data that is not protected.

### ***Multiple Identifiers, examples***

An IoT device may have one identifier or a number of different identifiers that may be established at manufacturer or added prior to deployment. Identifiers can be used as part of the device onboarding process, or as part of ongoing device/application management. Each identifier must be unique in a namespace to allow it to be referenced without ambiguity. These identifiers link to various device identities needed for proper authentication and authorization of various functions for device operation and management. Note that in some cases device identity can be added, updated or changed post manufacture or deployment by authorized access.

#### ***Examples include:***

- ▶ **Device specific, embedded identifiers** associated with the physical hardware of a device, such as Layer 2 MAC addresses used to identify the device to an access network, or the International Mobile Equipment Identity (IMEI) or Mobile Equipment Identifier (MEID) of a cellular device.
- ▶ **Subscription based identifiers** that may be used to enable device access to WAN based network services. These include mobile International Mobile Subscriber Identity or IMSIs used for cellular network access.
- ▶ **IoT application identifiers** that allow an IoT application to identify and access devices for use. Each IoT application using a specific IoT device may have its own unique application identifier.
- ▶ **IoT device management system identifiers**, separate unique identifiers for management access to the devices under the management system's control or scope.
- ▶ **Asset tracking identifiers** such as Electronic Product Codes (EPC) and Tag Identifiers (TID); these are used to obtain track and trace information
- ▶ **Trusted certificates**, which may have a "Unique Name" that is different from all the above but should correlate to a known identity.

#### ***Identity/Identifier uses:***

Identity is the basis for trustworthiness. Each device should be able to generate, and/or store at least one identifier tied to Identity. The device identity is the building block upon which a broad range of security controls and device manageability depend for proper functionality.

Storage and usage of each of the device identifiers should be protected as appropriate for that identifier. For example, identifiers specific to the physical hardware should be saved in immutable storage components in the device. Provisionable identifiers should also be protected from unauthorized access, changes, and hacks.

### ***Examples of how Identifiers are used in Root of Trust***

A Root of Trust (RoT) is a component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. These devices/functions are ideally implemented in hardware, are tamper resistant, and create a walled off crypto compute environment that is only accessible via APIs from the device's general compute. For example, a unique secret key might be provisioned into the hardware “root of trust” function which is operated on by the isolated crypto functions. The IoT device never directly sees the underlying secret and never does any of the crypto processing itself.

The highest level of trust that a device can attain depends on the strength of the root of trust. The root of trust, or multiple roots of trust, in a device consist of hardware, software,<sup>18</sup> and other aspects that establish the confidence in the identity of the device or its services. By definition, all devices have one or more roots of trust, and the strength of the root of trust determines the level of confidence in the authenticity of the identifier(s). Much of security is dependent upon the authenticity of device or application identities. The requirement for the strength of the root of trust depends on the threat model and criticality of the device; critical devices may require a hardware root of trust while non-critical devices may suffice with software (or even less capable) root of trust.

Therefore, the hardware RoT is not a panacea, nor is it a viable solution in all devices. On the other hand, without secure storage with crypto capabilities one is effectively hanging the key on a hook next to the lock, so key storage requirements should be considered carefully. See also Section 5.1.4, *Data At Rest is Protected* regarding storage protection requirements.


It should be noted that characteristics that are unique to the device, including Device Identity, can have unintended or undesirable consequences when readable from a distance or over the internet. An example of such an undesirable capability is cyberstalking. Such a features should be configurable or replaceable by a person with local control of the device, particularly if the device can be potentially resold (see also Section 5.1.10 *Reprovisioning*).

## **5.1.2 Secured Access**

**Definition:** Protection of device operational and management capabilities by requiring user<sup>19</sup> authentication to read or modify the software, firmware and configuration, including means to ensure device-unique credentials for administrative access, and by protecting access to interfaces.

**Scope:** This capability includes authenticating authorized users for remote or local access to the operational and management capabilities (including software, firmware and configuration). Authentication may take different forms based on the risk profile of the device, and will depend on the application. It may include requiring a secure certificate from a trusted source, user credentials, biometrics, and/or multi-factor authentication. Authentication must follow good cyber hygiene practices, for example, prevention of default password abuse, device-unique passwords, rate-limiting on password attempts, first-time-change requirements on default passwords, and protection of stored credentials. Credentials should not be shared between users (i.e. there should a unique set of credentials for each user identity that is authenticated).





This capability also includes securing physical interfaces (e.g., debug ports or JTAG) as needed to ensure protection of the software, firmware and configuration. This capability does not include preventing or detecting physical access to the device.

---

**Discussion:** This item is intended to help protect the device software, firmware and configuration from unauthorized access either remotely or when a malicious actor has physical access. Note that some devices may not implement an administrative access feature, in which case access may be considered “secured” by this design choice.

A further note with regard to default credentials (e.g. default passwords or a shared certificate); when a non-unique default credential is provided, it should be required to be changed upon first use, or may not be used to provide modification of sensitive parameters.

### 5.1.3 Data In Transit Is Protected

---

**Definition:** Protection of the confidentiality and integrity of selected categories of transmitted data via sound cryptographic means, e.g., HMACs, TLS/DTLS, IPsec, or SSH.

---

**Scope:** This capability involves certain data exchanged between the device and other devices, gateways/hubs, and the general internet. An important element of scope is the selection of which data is to be protected; the selection is use-case-specific and should be based on a risk assessment for the device and usage. Note that the user may have some control (settings) over what and whether data is protected in transit.

---

**Discussion:** Some devices gather data of little importance or with little temporal value; not all data needs to be protected. Protection may also imply different security properties. For example, confidentiality may be paramount for some data while integrity may be more important for something else. The need and type of protection may be determined based on the data being collected, the context of collection, and other risk factors.

Regardless of data handling policies, certain classes of data should always be protected. For example, data related to the security of the device or system, such as identity and credentials that support that identity (i.e. the configuration) should not be communicated in the clear. Additionally, updates to the software and firmware should also be protected.

Some devices only have internet access via a hub. In those cases, it is important to consider the security of the hub itself, because if the hub does not have baseline security capabilities the device is effectively open to compromise via the hub. It is also important to note that there are low-level or low-capability devices that have limited resources; however, some level of data protection may need to be implemented.

It should be noted that certain types of information—sometimes referred to as “personal”, “sensitive”, or “personally identifiable” information—are subject to rules regarding protection under applicable law and regulation and therefore must be evaluated for protection under those legal frameworks. However, defining “personal”, “sensitive”, or “personally identifiable” information and the required protections are beyond the scope of this document.



Unprotected passwords and unprotected cryptographic keys must always be protected when sent over a public or shared medium.

### 5.1.4 Data At Rest Is Protected

**Definition:** Protection of the confidentiality and integrity of selected categories of stored data via sound cryptographic means.

**Scope:** Data that is stored on the device that, if compromised, would enable attacks at scale such as botnet attacks.

**Discussion:** This topic requires a certain amount of balance. While the most conservative approach would be to declare all data as worthy of protection without exception, the extreme challenge of such a broad requirement indicates that a use-case evaluation is more appropriate at this time.

While other security concerns should be addressed, it is appropriate to deal with the largest problems—attacks at scale—with the greatest priority. The possibility that a device model can be widely deployed and widely compromised for massive DDoS attacks and social media campaigns is a critical risk.

The possibility that a device model could be compromised is independent of industry and application. Therefore, it is appropriate to discuss this as a baseline capability but also to limit the application of this capability to those devices that have the capacity to be compromised at scale and used in a botnet.


This capability applies to devices with the following key characteristics:

1. The device can be communicated with via the general internet, including behind NAT, using well-known internet protocols
2. The device has an expected useful life (when connected) more than a few days or weeks (this criterion is intended to exclude devices with a very short post-market lifetime, such as package delivery tracking smart labels or tags).

If the device has the above key characteristics, cryptographic measures must be taken to ensure protection of data that, if compromised, would enable attacks at scale such as botnet attacks. Such protective measures should include ensuring the integrity of stored code. Code insertion by an attacker is a common technique of botnet infections and other attacks at scale.

System credentials or keys, user credentials and user data stored on the system should be protected for confidentiality when compromise of this data facilitates attacks at scale. Requirements for user credentials noted in Section 5.1.2 *Secured Access* provide guidance to ensure that user and system credentials are device unique and as such, mitigate their use in such attacks

When protecting the integrity or confidentiality of data, Section 5.1.1 *Device Identifiers* addresses the topic of the RoT which should be considered when implementing Data-at-Rest protection.



Elements of Data-at-Rest may or may not be subject to law or regulation; this must be determined by the type of data stored.

### 5.1.5 Industry Accepted Protocols are Used for Communications

---

**Definition:** Use of secure, widely used protocols, excluding deprecated and replaced versions and protocols, for communications to and from the device.

---

**Scope:** Protocols used in exchanging data between the device and other devices; cryptographic standards may sometimes be thought of as “protocols” but are considered separately (see Section 5.1.8, *Cryptography*).

---

**Discussion:** “Secure” here means that the protocol does not have a known vulnerability with a ready exploit. Another way to view this item is that it is about the use of security-aware and security-capable protocols for communications to and from the device. But it is important to recognize that even some traditionally accepted protocols may be deprecated now.

Therefore care must be taken in evaluating protocols used. As an example of an insecure implementation, one might “use” TLS 1.3<sup>20</sup> as the transport layer security but allow negotiation to settle on SSL 2.0, which has known vulnerabilities and is deprecated by the IETF<sup>21</sup>. Any such fallback must not result in the use of deprecated protocols.

One may also seek “accredited” protocols or “voluntary consensus standards”. In some countries, laws and regulations may limit some options, however. Open, published and peer-reviewed protocols may not be accredited voluntary consensus standards, but at least have had their details reviewed by experts. Where feasible, of course, international or regional voluntary consensus standards are generally best.

### 5.1.6 Data Validation

---

**Definition:** Parsing and limiting input data to prevent it from being used directly as code, commands, or other execution flow inputs; and encoding output data in a form appropriate to and limited to its intended usage.

---

**Scope:** This capability applies whenever a device accepts user input, for example for human-readable text fields in a management console.

---

**Discussion:** This capability is intended to prevent the large category of exploits that may be available when input data includes special characters or otherwise is conditioned to abuse the data handler. One common type of such exploit is the cross-site scripting (XSS) exploit.<sup>22</sup>

For example, when restoring configuration settings to a device by uploading a saved configuration state, the file “../permissions.bin” might be uploaded to overwrite access parameters; stripping “special” characters including the slash is a form of data validation.

Not all devices have data-handling features that would make data validation appropriate, but if they do include such a feature (such as a web interface for configuration), this is a large area for potential abuse.

Note that Section 5.1.2 *Secured Access* has some overlap in intent but has a separate scope.

### 5.1.7 Event Logging

**Definition:** A limited persistent record in the device of relevant events, secured and available to authorized users.

**Scope:** This capability has to do with recording attempts to access the device configuration and other relevant security events. A device needn't keep an infinite number of records and may make use of a simple ring buffer depending on storage limitations. "Relevant events" are device-specific but may include detection of incorrect boot time, failed hash check, or excessive failed login attempts.

Where the device uses a hub or gateway to connect to the internet, the hub or gateway may provide this capability on behalf of the device. This capability is conditioned on the assumption that there is a reasonable likelihood of log inspection for the device type.

**Discussion:** Logging is a basic need both for forensic analysis, and for real time understanding of system failures. When something goes wrong, it is important to understand what chain of events led to a failure, and what devices are impacted. Logging to an external system is desirable, but not required. Use of standards such as syslog limits storage requirements. However, any mechanism that can provide some indication of anomalous behavior to the administrator — either in real time or retrospectively — is desirable.

### 5.1.8 Cryptography

**Definition:** Where cryptography is used, use open, published, proven, and peer-reviewed cryptographic methods with appropriate parameter, algorithm and option selections.

**Scope:** The technical means used to ensure confidentiality, integrity, and authenticity of data; the technical means used to verify authorization and ensure non-repudiation.

**Discussion:** Do not implement "home-grown" cryptography. Good cryptography is difficult. It is considerably more difficult when using proprietary solutions. Cryptographic methods should be chosen to match the assessed risk but should use open, proven, peer-reviewed methods and algorithms with—ideally—updateability<sup>23</sup> or the ability to use new cryptographic algorithms.

The purpose of cryptography is to ensure confidentiality, integrity and availability. Example uses may include protecting data in transit (outside the device and in certain cases within the device), protecting data at rest, authentication, authorization, etc. Determining the data to be protected requires some judgement; see related



sections. However, examples of such data may include sensitive data (credentials, etc.) and user defined data (PII, access credentials, etc.)

Note that in some areas the cryptographic methods may be limited to a certain approved set. Within that approval space, the developer should use the best available.

### 5.1.9 Patchability

---

**Definition:** The ability to verifiably update a device’s software and firmware, post-market, with patches that are authenticated to ensure that they have been deployed by an authorized entity as well as to verify the integrity of the patch.

---

**Scope:** The patchability capability will vary with device complexity, manageability, and use case. For example, it may not be necessary for all devices to support download of software patches from a remote location; however, such a capability may be the most feasible approach to patch management for all device categories.

Note that some IoT devices are designed to be useful for very short periods of time, after which their purpose is complete and they are removed from service. Examples of such throw-away devices might include disposable smart shipping labels and disposable smart medical bandages.

For such devices, exploits should be patchable pre-market and applicable company policy should determine effective mitigations post-market. To further limit the risks posed by un-patchable “throw-away” devices, the device provider should have a mechanism to identify vulnerable devices, disable vulnerable devices, and communicate the need for replacement of vulnerable devices to end-users.

Note that acknowledgement of such “throw-away” devices does not provide an option to omit patchability by simply declaring a device to have a short lifetime. The patchability capability is intended to be for a reasonably useful period post-market.

---

**Discussion:** This capability can be quite difficult from a technical and feasibility point of view. However, it is clear that patchability is necessary in today’s world, unless the device will be taken offline or decommissioned when an update is not possible. Over-the-wire or over-the-air and automated patching for connected devices is preferred to more manual means.

Devices should have the ability to validate patches and ensure that they are unmodified and have not been tampered with. The patch should not reset the settings of the IoT device. Where feasible, using a cryptographic data origin authentication mechanism (e.g., a digital signature or (H)MAC) to protect the patch and validate that it has not been modified is appropriate. Application (or code) signing, where applicable, should also be considered.

### 5.1.10 Reprovisioning

**Definition:** The ability for authorized users to securely reconfigure and redeploy a device post-market, especially to return the product to factory defaults or an authorized restore point, and securely remove data collected by the device (that is not essential to its operation), within a defined period established by the organization.

**Scope:** This capability applies to the device configuration, including the initial “as-shipped” configuration, any additional pre-set configurations available to users, and the “as-used” configuration after the device is deployed. See the definition of “configuration” in Section 2, *Definitions and Acronyms*.

**Discussion:** In the Definition of this capability, the phrase “securely remove” does not have a widely agreed upon definition, and may vary; it may be an action defined by organization policy commensurate with risk that may leave the device in a default/factory-fresh state or other defined state.

Note that, depending on device hardware details, simply wiping memory may or may not be sufficient. Or it may be sufficient to erase memory allocation tables in some devices, but not in others.

Although use of a ‘reset command’ may allow for the easy reset of a system, the implementation of such a command may allow for remote denial of service attacks, or similar exploitations. Therefore, consideration of the risk environment of the system must be made prior to deploying any such solution. A device capability to restore to factory settings is appropriate and should have multiple security protections for managed IoT devices deployed at scale (e.g., smart city deployments) and support the corresponding protection mechanisms.

## 5.2 PRODUCT LIFECYCLE MANAGEMENT CAPABILITIES - BASELINE

This section considers the important capabilities that are in scope for the organization, rather than the device. Device capabilities are typically observable on a given device. These product lifecycle management capabilities are activities of the manufacturing organization (or otherwise responsible development organization) that are important in the context of overall security of the device.

### 5.2.1 Vulnerability Submission and Handling Process

**Definition:** A defined and managed process for accepting vulnerability notifications and acting on them.

**Scope:** This is a business and engineering process capability for handling information related to software vulnerabilities, interacting with internal staff and external parties who are part of that information flow, and actually addressing the vulnerabilities themselves.





---

**Discussion:** The capability to handle vulnerabilities does not imply transparency. Vulnerability transparency is a policy or management action regarding notifying users of known vulnerabilities.

Vulnerability handling should be done in a timely manner, based on prioritization. Upon identification, vulnerabilities should be evaluated in terms of risk, scope of affected products, availability of mitigations, and other factors, and should be prioritized based on that evaluation. Organizations should allocate resources to address identified vulnerabilities according to that prioritization.

“Accepting vulnerability notifications” can be done in various ways. For example, an organization can participate in threat sharing programs, review posted threat information, work directly with third parties or publish information on how to reach a security team’s defined point-of-contact.

With regard to a security team’s defined point-of-contact, a useful “default” is security@company.com, where company.com is the organization’s email domain. Many third parties will attempt to contact an organization through this path. Despite this default’s popularity, however, the organization should have a “landing page” for contact information and policy on handling vulnerabilities.<sup>24</sup>

## 5.2.2 EoL/EoS Updates and Disclosure

---

**Definition:** A defined manufacturer policy covering the handling of any post end-of-life (EoL) or end-of-service (EoS) device vulnerabilities, if and how updates will be available, and what to do with the device at EoL/EoS.

---

**Scope:** The published manufacturer policy on end of life and end of service.

---

**Discussion:** This capability must be considered carefully within the organization. It is tied to vulnerability handling, the product lifecycle, terms of service and more.

## 5.2.3 Device Intent Documentation

---

**Definition:** An explanation of the device’s as-designed network usage that is made available by the manufacturer publicly, in product documentation, or other means for device users.

---

**Scope:** Device use of network resources including communication with other devices; use of internet resources (including web sites); and with what protocols or services (e.g. UDP/TCP).

---

**Discussion:** The manufacturer or other responsible organization publishes, in a place readily accessible to device owners and operators, a summary of what behavior to expect from the device. An IoT device that is not intended to be on social media, or to scan port usage on the local intranet, or to contact devices made by other manufacturers, should not do these things. However, it is not always clear to the human monitoring the network whether a particular behavior is anomalous or not. The documentation should clarify this point. The user (or device administrator) should be able to readily determine what this device is intended to communicate with in terms of other devices; internet resources (including web sites); and with what protocols or services (e.g. UDP/TCP) as per the Scope.

It must also be noted that many device owners will not choose to use this information or may not have the training or experience necessary to use this information. However, it is important that the information be made available to those who can use it.



## 05 | Annex A: Regarding Future Secure Capabilities — Phase in Over Time

The following items are considered significant enough that they should be baseline capabilities. However, for various reasons they cannot be considered baseline at this time. The expectation is that they will become baseline and developers should carefully consider the capabilities in their planning.

### A.1 Device Intent Signaling

---

**Status:** Baseline Capability to Phase In over Time

---

**Definition:** Means for the device to provide information to routers or firewalls upstream what kind of traffic the device was intended to produce.

---

**Scope:** This capability includes device-provided heuristics related to the device in normal operation (so that network analysis can be performed) and can include protocols such as Manufacturer Usage Descriptor (MUD)<sup>25</sup>, OMA-DM<sup>26</sup> and TR-69<sup>27</sup> (the latter two being applicable in cases where the devices can be managed directly), security requirements including Open Connectivity Forum Security Profiles (Black, Blue and Purple), and proposals such as IoTSense.<sup>28</sup>

---

**Discussion:** This capability will have a significant effect to reduce the scope and spread of botnets. There are test and implementation projects<sup>29</sup> under way to verify some of these technologies as well as discussions regarding appropriate use cases. Other voluntary consensus standards may be applied for similar capability.

It may also be helpful for the device to have its intent defined in a public way. As an example, a device manufacturer could simply have a published MUD file, regardless of whether the device supports emitting the URL or the network enforces the resulting intent. Knowing the device intent—even if it is simply via a plain text file as to what the device does—can help those seeking to correct anomalous behavior or reduce device threat surface.

Because the core technologies are documented but in testing, or available but not documented to this specific intent, this capability is considered one that should be phased in over time.

### A.2 Device Network Onboarding

---

**Status:** Baseline Capability to Phase In over Time

---

**Definition:** Means to enable a network operator or device manager to cryptographically ensure that a device, when first attached to a network, is identified, authenticated and authorized.

---

**Scope:** Device onboarding is the process of authenticating the device, authorizing that device with credentials, and configuring it to be able to communicate within the security domain under question.

---

**Discussion:** From a security perspective, this process is one of the exchanges most fraught with peril. Correct identification of the device, and explicit, non-automated, approval from the network manager are both critical to the exchange.

**Examples of Device Provisioning Protocols include the WiFi Alliance Device Provisioning Protocol (DPP).**

**Examples of Onboarding can be found in the OCF specifications.**



## 06 | Annex B: Additional IoT Device Security Capabilities and Practices

This section identifies capabilities or practices that are not broadly applicable across the diverse IoT ecosystem and are therefore not intended to be part of the baseline. This does not mean that these capabilities are not important in the effort to secure the IoT ecosystem; it simply means that they are not suitable for a broad baseline.

### B.1 Secure Development Lifecycle

---

**Status:** Not a Baseline Capability

---

**Definition:** Use of software assurance processes that consider security throughout the design, deployment, integration, and maintenance of software to reduce the risk of vulnerabilities and weaknesses.

---

**Scope:** A secure software development lifecycle (SDL) is a set of guidance and processes designed to ensure security considerations are addressed throughout the software's lifecycle. While specific elements of an SDL may vary, SDLs should include, at minimum, the following elements:

1. Processes to identify likely threats to the software and to map security controls and other mitigations to those threats in designing the software;
2. Processes to ensure that software code is written according to established voluntary consensus coding standards and avoids common weaknesses and vulnerabilities;
3. Processes to identify, vet, manage, and securely integrate third-party software components;
4. Processes to test and validate software security controls and capabilities; and
5. Processes to identify, manage, mitigate, and learn from new vulnerabilities, weaknesses, and advancements in best practices.

---

**Discussion:** Many IoT device manufacturers use software developed by third-parties; the intent of this item is to ensure that IoT device manufacturers obtain software components from software developers that have SDLs in place, and that manufacturers are able to obtain information from software developers about the nature and scope of their SDLs.



### B.2 Hardware Rooted Security

---

**Status:** Not a Baseline Capability

---

**Definition:** The starting point of a chain of trustworthiness that includes a trusted execution environment with cryptographic functions, runtime execution tamper protection and an interface for the host process of the device.

---

**Discussion:** Hardware rooted security is important for certain aspects of security, but not all devices require it. Elements of hardware rooted security may include,

Secure or measured boot process. A secure boot process ensures that only the intended boot software is run. A measured boot process can signal an anomaly if other boot software is run because the boot process metrics will differ.

Protected or hardware cryptographic keys, which may be used to authenticate boot components or to uniquely identify the hardware device. A hardware-based key may also be used as a private key for software or application decryption. Multiple keys are typically required for the various purposes.

Trusted execution environment, which has access to reserved software and data for security purposes.

### B.3 Time Distribution

---

**Status:** Not a Baseline Capability

---

**Definition:** Means to synchronize the device internal clock to wall clock time (e.g., UTC or “GPS time”).

---

**Discussion:** Time awareness could be an element of using good cryptographic methods; that is, some details of a secure device may need a reliable time indicator. For example, for logging of events, a known good timestamp is important.

However, implementing time distribution as a component of an overall cryptographic strategy or architecture implies that the time distribution protocol itself is a secure process. Time packets must be cryptographically signed for authentication to prevent man-in-the-middle attacks. If the time distribution protocol is used to manage key expiration, message spoofing can be a problem. See <http://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf> for a discussion of security concerns for the NTP time distribution protocol.

### B.4 System Resiliency

---

**Status:** Not a Baseline Capability



---

**Definition:** Ability to maintain service in the presence of certain kinds of faults.

---

**Discussion:** This capability is related to the principle of “least functionality”. This is a best practice. A device must be able to function post security attack (assuming the attack did not result in actual damage); however, the device may require software or firmware reinstatement or update.

The types of faults that may occur, and to which the device should be resilient include power outage or network outage; the latter includes specific network resource outage or unavailability such as the inability to contact a server or website. On resumed availability of power, network or resource, the device should be able to return to operation in a stable state.

## B.5 Secure Toolchains

---

**Status:** Not a Baseline Capability

---

**Definition:** A set of programming tools to perform or automate large parts of the software development process that are designed and employed with security of the final product in mind.

---

**Discussion:** The toolchain is the suite of software tools used to develop, compile, build and maintain a software product, including the software or firmware embedded in an IoT device. Security-focused toolchains provide the capability to check if the implementation is following secure coding guidelines and to search for a subset of known Common Vulnerabilities and Exposures (CVEs) in the open source software.

Tools such as fuzzing, symbolic execution, sandboxing, static and dynamic analysis, and memory-safe languages can also be used to find and mitigate vulnerabilities.<sup>30, 31</sup>

## B.6 Software Transparency and Bill of Materials

---

**Status:** Not Baseline Capability

---

**Definition:** Ability to expose information about the software components used to build the device, including the components and their provenance.

**Discussion:** This capability is considered important, but currently the state of the art appears unready for Baseline status.

Software transparency refers to providing information regarding the sources of the devices software or firmware. The software bill of materials is an inventory of the device’s current internal software and firmware including versions and patches.<sup>32</sup>

However, these features are still evolving and not fully available. For reference, note that NIST says in their *Considerations for a Core IoT Cybersecurity Capabilities Baseline* that software transparency “may offer utility [but] would be difficult to adequately verify and harder to implement”. They further note that the SBOM capability “is useful for update management but not necessary in all update mechanisms.”<sup>33</sup>

There are technologies and products available, and requirements in certain markets, but these capabilities are not considered baseline.

### B.7 Least Functionality

---

**Status:** Not a Baseline Capability

---

**Definition:** Ensuring that the device has only the necessary functions for operation.

---

**Discussion:** This is a good best practice but not a Baseline. Generally, it cannot be shown that a device exhibits least functionality, and at best a developer can only assert that they practice this during development.

### B.8 Physical Access Control

---

**Status:** Not a Baseline Capability

---

**Definition:** Means to prevent a malicious actor from gaining undetected physical access to the unit, including tamper seals, conformal coating and physical locks.

---

**Discussion:** Physical access control is helpful to deter certain kinds of attacks. In many use cases, however, it is a consideration for the installer. Developers may consider tamper resistant coatings or tamper evidence seals.

### B.9 Best Current Practices

---

**Status:** Not a Baseline Capability

---

**Definition:** Use of recommended industry practices and voluntary consensus standards.

---

**Discussion:** Best practices are important and should be considered by the developer and the organization.

However, this capability cannot be verified on the device.

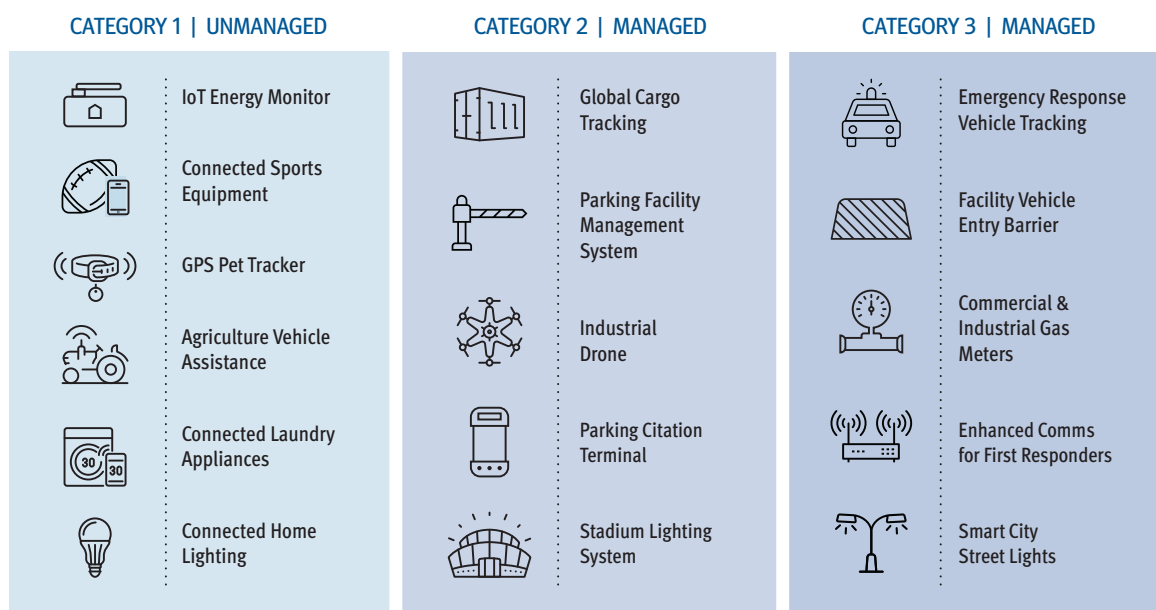
## 07 | Annex C: Discussion of Implementation and Complexity

The Baseline Capabilities described in the preceding sections can be implemented with various technologies, generally specified in voluntary consensus standards documents. Because there are options for each Capability, selection of the appropriate technology and appropriate implementation details (such as parameters or options) is critical. This section describes how to categorize device types to map to the appropriate levels of complexity in the implementation of the Baseline Capabilities.

As a common reference point, consider three categories of devices:

1. Category 1 devices are **low-complexity, unmanaged** devices (e.g., connected light bulb, connected appliances);
2. Category 2 devices are **medium-complexity, managed** devices (e.g., Industrial Drone, Global Cargo Tracking System);
3. Category 3 devices are **high-complexity, managed** devices (e.g., connected gas meter, connected city street lights).

**FIGURE 1: USE CASE EXAMPLES**



While it is critical that each of these types of devices is secure, they each require different security features because they have different degrees of complexity and manageability, and different use cases, which all result in different risk profiles. What is appropriate in an emergency response vehicle tracking system may not be appropriate in a GPS pet tracker.

Similarly, while some Baseline implementation methods or technologies are appropriate for Category 2 and Category 3 devices, they may be inapplicable to Category 1 devices. This does not mean that these features are not important in the effort to secure the IoT ecosystem; it simply means that they are not suitable for a broad Baseline. With this flexibility, the Baseline is appropriate for and applicable to all new IoT devices, even those at the lowest end of the complexity, sophistication, and manageability spectrum—like a connected light bulb.

By taking this approach—creating a Baseline for all new IoT devices, as opposed to creating a Baseline that is only relevant for complex or managed devices—the goal is to help to lift cybersecurity for the entire Internet of Things, including the network to which all of these devices connect.

### ***Use Case Examples Where Complex Capabilities Are Not Appropriate***

Encryption of all data at rest is a key example of a requirement that is not well-suited to all new IoT devices. In many instances, the data that would be protected is not sensitive or is less likely to be susceptible to misuse or danger if improperly accessed so that the tradeoffs for encrypting the data—including increased impacts on processor and decreased battery life—are high. As such, setting a baseline that expects all data at rest to always be encrypted in all IoT devices is fundamentally at odds with pragmatic risk management.

A few examples illustrate this:

- ▶ Adding encryption-at-rest to a GPS dog collar that has Wi-Fi or LTE connectivity will severely impact the battery life in that device. This tradeoff might make sense in some use cases, but it does not make sense with a low-complexity dog collar, which provides limited useful data.
- ▶ For IoT elements like low complexity sensors, where data is temporal or ephemeral, requirements to encrypt data at rest are unnecessary and burdensome.
- ▶ Connected footballs, soccer balls, and golf clubs may give users performance data from gyros embedded in them; however, on balance this is not the type of data that is likely to need to be encrypted at rest, and in fact, encrypting the data that is stored by these devices may degrade the utility of the device itself due to processor load.

Similar arguments can be made that other complex capabilities should not be treated as universal baselines, even if they may be desirable in many (or even most) use cases.

Many of these complex features are appropriate for other types of devices, namely Category 2 and Category 3 devices. The key is that beyond an agreed and basic universal baseline, there is not a one-size-fits-all solution: features to implement these capabilities should be determined based on the device's risk profile, which is informed by the device's complexity, sophistication, manageability, and general use case. For example,





- ▶ The risk profiles of general cargo tracking devices at sea, on rail, or on the road may call for specific security features, whereas a tracking device that monitors emergency response vehicles may call for other security features.
- ▶ The same logic would apply to a small stadium lighting system that needs to be connected to a school and a connected city lighting system that can dynamically adjust to multiple conditions depending on 911 calls, the presence of people in an area, gunshot detection technology, etc.
- ▶ A parking facility system may need added security because it combines entrance and exit with a point of sale terminal, while a high security entrance to a prison, an energy plant, or a military base would need even further enhanced security systems and added cybersecurity controls.

NIST has acknowledged that “[b]ecause IoT devices and their uses and needs are so varied, few recommendations can be made that apply to all IoT devices.” NISTIR 8228 DRAFT, <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf>.

Because of this, a Baseline needs to be truly focused on those few Capabilities that are really universally applicable. Further, the implementation of this Baseline is subject to risk/complexity/management tradeoffs based on the risk, complexity and managed/unmanaged nature of the device type and application.

## 08 | Annex D: Informative References

The work of the C2 Consensus organizations draws on recommendations by these groups and others. The following references are informative.

- ▶ [IABG] Council to Secure the Digital Economy (CSDE), “*International Anti-Botnet Guide*”, November 2018, <https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf>
- ▶ [CTIA IoT CC] CTIA, *Cybersecurity Certification Test Plan for IoT Devices*, October 2018, [https://api.ctia.org/wp-content/uploads/2018/10/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1\\_O\\_1.pdf](https://api.ctia.org/wp-content/uploads/2018/10/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_O_1.pdf)
- ▶ [ETSI] European Telecommunications Standards Institute (ETSI), *TS 103 645 Cyber Security for Consumer Internet of Things*, February 2019, [https://www.etsi.org/deliver/etsi\\_ts/103600\\_103699/103645/01.01.01\\_60/ts\\_103645v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf)
- ▶ [ENISA] European Union Agency for Network and Information Security (ENISA), *Baseline Security Recommendations for IoT*, November 2017, <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>
- ▶ [GSMA] Global System for Mobile Communications Association (GSMA), *GSMA IoT Security Guidelines for Endpoint Ecosystems*, February 2016, <https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf>
- ▶ [Security Pledge] Internet of Secure Things (IoXT), *The IoXT Security Pledge*, <https://www.ioxtalliance.org/s/ioXt-SecurityPledge-booklet-final.pdf>
- ▶ International Society of Automation (ISA)/International Electrotechnical Commission (IEC) — 62443 series of standards on the cyber security of industrial automation and control systems, <https://www.isa.org/isa99/>
- ▶ National Institute of Standards and Technology (NIST, United States Department of Commerce), *Considerations for a Core IoT Cybersecurity Capabilities Baseline*, February 2019, [https://www.nist.gov/sites/default/files/documents/2019/02/01/final\\_core\\_iiot\\_cybersecurity\\_capabilities\\_baseline\\_considerations.pdf](https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iiot_cybersecurity_capabilities_baseline_considerations.pdf)
- ▶ [NISTIR 8259] National Institute of Standards and Technology (NIST, United States Department of Commerce), NISTIR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*, July 2019, <https://csrc.nist.gov/publications/detail/nistir/8259/draft>
- ▶ [OCF Security Specification ISO/IEC 30118-2:2018] Open Connectivity Foundation (OCF), *OCF Security Specification 2.0.1*, February 2019, [https://openconnectivity.org/specs/OCF\\_Security\\_Specification\\_v2.0.1.pdf](https://openconnectivity.org/specs/OCF_Security_Specification_v2.0.1.pdf)
- ▶ [DCMS] United Kingdom Department for Digital, Culture, Media and Sport (UK DCMS), *Code of Practice for consumer IoT security*, October 2018, <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iiot-security/code-of-practice-for-consumer-iiot-security>
- ▶ [UL] UL, UL MCV 1376 — Security Capabilities Verified, <https://shopulstandards.com/ProductDetail.aspx?UniqueKey=35953>
- ▶ World Wide Web Coalition (W3C), *WoT Security Best Practices*, retrieved May 2019, <https://github.com/w3c/wot-security-best-practices>
- ▶ World Wide Web Coalition (W3C), *WoT Security Testing Plan*, retrieved May 2019, <https://github.com/w3c/wot-security-testing-plan>

## 09 | Annex E: Mapping to CSDE International Anti-Botnet Guide

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	[IABG] 5.C.3: Where possible, the device should support network asset management by enabling the ability to identify and audit the device logically and physically and with proper access control.
Secure Device Capabilities - Baseline	Secured Access	[IABG] 5.C.1.b.2: Unique "admin" credentials per device or a first-boot requirement to change passwords Rate-limiting techniques to prevent brute-force password guessing Securing or disabling developer-level ports and services prior to product shipment Removing unused or insecure local and remote administrative services such as telnet. Multi-factor authentication user access control should be supported.
Secure Device Capabilities - Baseline	Data In Transit Is Protected	[IABG] 5.C.1.b.1: Data communications should be encrypted. Regardless of whatever protocols are in use, if authentication is available, it should be used. In general, the security mechanisms available in whatever system is used should be employed.
Secure Device Capabilities - Baseline	Data At Rest Is Protected	[IABG] 5.C.1.b.1: Sensitive data should be stored encrypted. In general, the security mechanisms available in whatever system is used should be employed.
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	[IABG] 5.C.1.b.1: The latest versions of protocols and security mechanisms should be used. Secure memory can be used in lieu of encryption for stored information. Encryption key methods comporting with NIST FIPS 140-2 or ISO/IEC 24759 should be used.
Secure Device Capabilities - Baseline	Data Validation	[IABG] 5.C.1.b.4: Any input received from outside the system must be managed so that an outside adversary cannot take advantage of unintended consequences. Input should be validated for length, character type, and acceptable values or ranges; see also whitelist filtering. Output from one subsystem to another or to another site should also be filtered; see "character canonicalization."
Secure Device Capabilities - Baseline	Event Logging	
Secure Device Capabilities - Baseline	Cryptography	[IABG] 5.C.1.b.1: Cryptographic techniques used should avoid deprecated methods. [IABG] 5.C.1.b.5: Cryptographic methods are required to ensure data integrity and confidentiality, rights authentication and non-repudiation of requests. This cryptography should be chosen to match the assessed risk but should use open, peer-reviewed methods and algorithms. Where feasible, cryptographic methods are updateable. ([IABG] Advanced section: Strong, proven, updateable cryptography using open, peer-reviewed methods and algorithms. Ensure cryptography has the ability to support post-quantum resistant key lengths for symmetric encryption.)

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Patchability	[IABG] 5.C.3: May provide notice to the consumer about security support policy and how the device is supported with updates during and what to expect after the support period. ([IABG] Advanced section: A plan for secure updates with anti-rollback protection and proper access control throughout a defined security support period, where technically feasible.)
Secure Device Capabilities - Baseline	Reprovisioning	[IABG] 5.C.3: After the support period, consumers should have the ability to and be informed about how to “decommission” the device. Decommissioning should allow a consumer to return the product to factory defaults and remove any Personally Identifiable Information (PII). This capability covers a variety of scenarios such as the sale, abandonment, or recycling of the product, including selling a property with IoT devices installed.
Product Lifecycle Management	Vulnerability Submission and Handling Process	[IABG] 5.C.3: Providers should create a security vulnerability policy and process to identify, mitigate, and where appropriate, disclose known security vulnerabilities in their products.
Product Lifecycle Management	EoL/EoS Updates and Disclosure	[IABG] 5.C.3: May provide notice to the consumer about security support policy and how the device is supported with updates during and what to expect after the support period.
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	[IABG] Multi-factor authentication user access control should be supported. IETF Manufacturer Usage Descriptor (MUD) may be supported; IEEE 802.1AR and the Device Identifier Composition Engine (DICE) should be considered to improve the security of the IoT device and its MUD components.
Secure Capabilities - Phase In Over Time	Device Network Onboarding	
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	[IABG] 5.C.1.a.1: A responsible company may have the secure development lifecycle (SDL) process. In the SDL process, each development phase has security activities that can be done manually or automatically. ([IABG] Advanced section: After establishing a secure development lifecycle process, the advanced company is measuring and growing process capabilities.)
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	[IABG] 5.C.2.a.1: Consider how hardware-rooted security fits into the secure development lifecycles of current and future products. ([IABG] Advanced section: Hardware-rooted security is utilized where technically feasible.)
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	



CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	[IABG] 5.C.4: A responsible company may have tools that are able to check if the implementation is following secure coding guidelines and to search for a subset of known Common Vulnerabilities and Exposures (CVEs) in the open source software. ([IABG] Advanced section: Tools such as fuzzing, symbolic execution, sandboxing, static and dynamic analysis, and memory-safe languages are used to find and mitigate vulnerabilities.)
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Current Practices	



## 10 | Annex F: Mapping to CTIA IoT Device Cybersecurity Certification

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	[CTIA IoT CC] 4.13 Device Identity is globally unique and required. Additional network components like a SIM/eSIM and MAC address are additional to the Globally Unique ID requirement. Additionally, device must provide its globally unique identity in the audit log
Secure Device Capabilities - Baseline	Secured Access	<p>[CTIA IoT CC] 3.2: Password Management Test - Unique Default Password for each device</p> <p>Password Change required upon first login</p> <p>Password is of sufficient complexity and length</p> <p>[CTIA IoT CC] 3.3: Authentication Test - Authentication required to modify device settings</p> <p>[CTIA IoT CC] 3.4: Access Controls - Role Based Access Controls</p> <p>[CTIA IoT CC] 4.2: Password Management Test - Idle logout</p> <p>Password Integration with Enterprise Management System</p> <p>[CTIA IoT CC] 4.3: Access Control - Integrated password with Enterprise Management System</p> <p>[CTIA IoT CC] 4.9: Multi-factor Authentication - Multi-Factor Authentication is supported</p> <p>[CTIA IoT CC] 5.17 Designed In Feature - All Network Communications except those minimally required to function are disabled by default</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[CTIA IoT CC] 4.8 Encryption of Data in Transit - Required support for TLS, DTLS, SSH or IPSec for end to end encryption at minimal 128-bit AES.</p> <p>[CTIA IoT CC] 5.15 - Encryption of Data at Rest - Required support for encryption of data at rest at minimal 128-bit AES</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[CTIA IoT CC] - CTIA recommends common peer reviewed industry standards</p> <p>Encryption in transit supports IPSEC, SSH, TLS and DTLS at the 128-bit AES support</p> <p>Encryption at Rest support ts minimal 128-bit AES support</p> <p>Digital Signature Generation and Validation support RSA or ECDSA algorithms for X.509 certificates in P7S formats</p>
Secure Device Capabilities - Baseline	Data Validation	<p>[CTIA IoT CC] 3.2 - validates inputs for password</p> <p>[CTIA IoT CC] 3.5/3.6 - validates patches and upgrades</p> <p>[CTIA IoT CC] 5.13 - validates digital certificates</p> <p>[CTIA IoT CC] 5.17 - validates network services minimally required</p>
Secure Device Capabilities - Baseline	Event Logging	[CTIA IoT CC] 4.7 Audit Log - Devices are required to handle 4 specific audit log type entries based on Syslog format. The four are emergency, alert, critical, and error audit log entries.

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Cryptography	<p>[CTIA IoT CC] 4.8 Encryption in Transit support minimally the 128-bit AES standard to protect data and support compatibility with the rest of IT ecosystem. It also supports strong, industry vetted protocols for end-to-end encryptions such as SSH, TLS, DTLS, and IPSec</p> <p>[CTIA IoT CC] 5.14 Digital Signature Validation and Generation supports industry adopted standards such as the RSA and the ECDSA algorithms to support strong X.509 certificates in P7S format. This protects software and supports strong authentication</p> <p>[CTIA IoT CC] 5.15 Encryption at Rest support minimally the 128-bit AES standard to protect data at rest and support compatibility with the rest of the IT ecosystem.</p>
Secure Device Capabilities - Baseline	Patchability	[CTIA IoT CC] 3.5 & 3.6, 4.5 & 4.6 Patches and Upgrades are a required element that is available at the lowest level from the manufacturer or at the managed level, provided by the managing enterprise infrastructure
Secure Device Capabilities - Baseline	Reprovisioning	
Product Lifecycle Management	Vulnerability Submission and Handling Process	[CTIA IoT CC] 3.1 Terms of Service and Privacy Policy - Manufacturers state how long a device will be support for patches and upgrades that will address vulnerability handling at the device level.
Product Lifecycle Management	EoL/EoS Updates and Disclosure	
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	[CTIA IoT CC] This is covered by most of section 4 in the plan regarding connecting the device to an enterprise management system. For cellular based devices, there is also a requirement to get the device provision through the operator.
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p>[CTIA IoT CC] 4.11 Secure Boot may be accomplished with the use of a hardware root of security such as a TPM module</p> <p>[CTIA IoT CC] 5.14 Digital Signature Generation and Validation may have a hardware root of trust module to support this functionality</p>
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	Suggest UL CAP program for this activity
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	[CTIA IoT CC] 5.17 - Designed-In Features - One requirement is that the device separate critical from non-critical functions. Another requirement is that the device fail in a secure manner.
Additional IoT Device Security Capabilities and Practices	Physical Access Control	[CTIA IoT CC] 5.16 Tamper Evidence - Devices at the CTIA Level 3 usually have secured if not hardened and weather rated enclosures meant to protect the device from case intrusion. As such, tamper evidence provides for silent notification if a case is opened and notification can be sent back to the network controllers
Additional IoT Device Security Capabilities and Practices	Best Current Practices	

## 11 | Annex G: Mapping to IoTopia Specifications

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	<p><i>Certificate based authentication. Onboarding requires a voucher with dev ID. MUD URL imbedded in device by manufacturer.</i></p> <ul style="list-style-type: none"> <li>a. Endpoints that communicate via IEEE 802 networking must contain a certificate (IDevID) along with the MUD-URL, and associated private key for the certificate. [IEEE802.1AR]</li> <li>b. Heuristics: Manufacturers must provide a description of device behavior that may be used by the network to infer identities</li> <li>c. Endpoints that implement via IEEE 802 networking must support installation of at least one local certificate (LDevIDs) and associated private keying material.</li> </ul>
Secure Device Capabilities - Baseline	Secured Access	<p>“Device must utilize secure standard protocols and security mechanisms to provide multi-factor authentication for remote and local (physical) access to device</p> <ul style="list-style-type: none"> <li>a. Devices should not be able to support full operation with default passwords</li> <li>b. secure password enforcement should be imbedded in device</li> <li>c. as appropriate, passwords will require updates”</li> </ul> <p>Prior to completing Onboarding (e.g. obtaining a local trust anchor and LDevID) Endpoints communicating on IEEE 802 networks MUST authenticate using their IDevID and must accept the local 802.1X network credentials without validation purely for the purposes of onboarding.</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p><i>Secure boot, secure data storage, measured boot, voucher storage, key storage, crypto support, crypto upgrade potential</i></p> <p>Endpoints must protect personally identifiable information from disclosure and modification. The actual implementation will depend on the nature of the endpoint and associated service, but an example would be to encrypt information on board the device such that only authorized users may access it.</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	<p><i>Device manufacturer should provide Heuristics related to the device in normal operation so that network analysis can be performed</i></p>
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p><i>Device must support industry standard protocols internally and for data transmission egress</i></p> <p>An Endpoint that communicates via IEEE 802 networking must support [RFC7030], Section 3 on TLS Layer, for certificate management of secure transport.</p> <p>Endpoints must measure secure boot: Secure boot is a ‘security mechanism’ and measured boot is the monitoring required</p> <p>Endpoints using IEEE 802.3 (wired Ethernet) must support [IEEE 802.1x] using the EAP-TLS [RFC5216] EAP method. Endpoints that have IEEE 802.11 transceivers MUST make use of [IEEE802.11] security in conjunction with [IEEE802.1X] (WPA Enterprise) to exchange [IEEE802.1AR] certificates</p>
Secure Device Capabilities - Baseline	Data Validation	

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Event Logging	Device must be able to log event and provide secure access to such logs to authorized users- lifecycle management
Secure Device Capabilities - Baseline	Cryptography	<p>a. Cryptography: The endpoint MUST support the SHA-256 hash algorithm</p> <p>b. The endpoint must support for Elliptic Curve Cryptography (ECC) described in [RFC6090] and [IEEE802.1AR] for use as LDevIDs</p> <p>c. An Endpoint must support either 2048-bit RSA certificates or ECC certificates as described in [RFC6090] and [IEEE802.1AR] for iDevIDs</p> <p>d. TLS Cipher Suite Support: Endpoints must minimally support the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite which is detailed within [RFC 7251] for EAP-TLS. This cipher suite will be used for the authentication operations used for both network layer and application layer authentication processes.</p> <p>RNG: An Endpoint must provide random number generation either through hardware or as compliant with FIPS 140-2 Sections 4.7.1 and 4.9.2.</p>
Secure Device Capabilities - Baseline	Patchability	<p><i>Device and manufacturer support secure SW/FW/HW updates throughout device lifecycle</i></p> <p>a. Endpoints must have the ability to securely receive and apply a software and/or firmware update</p> <p>b. All updates must be signed by the manufacturer, and Endpoints must validate signatures prior to applying any updates</p> <p>c. Endpoints that implement via IEEE 802 networking must support installation of at least one local certificate (LDevIDs) and associated private keying material</p>
Secure Device Capabilities - Baseline	Reprovisioning	<i>Device must support secure, authorized access control for remote and physical connection to device</i>
Product Lifecycle Management	Vulnerability Submission and Handling Process	<p><i>Manufacturer must provide any known device vulnerabilities and a plan or process to mitigate such vulnerabilities</i></p> <p><i>Endpoint manufacturers must have an active product incident response team (PSIRT), with documented processes and service level agreements, that customers and others can easily locate and call to report vulnerabilities.</i></p>
Product Lifecycle Management	EoL/EoS Updates and Disclosure	<i>Manufacturer should provide any EoL and end of support or EoS announcements in a timely manner to device owners. In addition manufactures should provide any expected vulnerabilities expected to E-o-Support (recommendations for mitigation)</i>
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	<p>Manufacturer must provide a file server that distributes Manufacturer Usage Description (MUD) files in accordance with MUD RFC</p> <p>a. The MUD-URL mustT be included in the client certificate used for a client authenticated 802.1X exchange. If an 802.1X service is not discovered by the client it mustT also present an unsecured statement of the MUD-URL via LLDP or DHCP</p> <p>b. Endpoints must only run applications or services whose TCP or UDP ports are described in the MUD profile</p>



CATEGORY	SUB-CATEGORY	MAPS TO
Secure Capabilities - Phase In Over Time	Device Network Onboarding	Device must support MUD URIs to provide the network with information to microsegment/set ACL's. In addition the device should support an automated onboarding capability such as BRSKI
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	<p>Vendors must have a written SDL process in place that includes the following elements at a minimum:</p> <ul style="list-style-type: none"> <li>• Training for software developers which includes secure coding techniques and requirements standard C libraries.</li> <li>• Threat modeling that includes a summary report of findings and a diagram.</li> <li>• Software security testing thru either dynamic or static analysis tools and a report that demonstrates testing was completed and output of testing.</li> </ul> <p>A way to document and track third party and open source components used in product. A summary of the vendor's specific SDLC process must be available on their public facing webserver.</p>
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p>Secure Storage: The Endpoint must contain its own certificate. The Endpoint must also contain the root certificate for the IDevID, Software Image Signing and Onboarding Services (MASA Root). Total of 4 certificates.</p> <p>Endpoints must store private keying material and certificates in tamperproof storage</p>
Additional IoT Device Security Capabilities and Practices	Time Distribution	<p>a. A trusted time source is necessary for the process of certificate validation and reliable system event logging and correlation. Endpoints MUST use either Simple Network Time Protocol (NTP) version 4 [RFC4330] or time provided by a trusted and authenticated server as described in Section 5.5</p> <p>b. Endpoints must periodically write the current time to non-volatile storage, and use that as a base prior to being configured with accurate time. The purpose of doing so is simply to prevent attackers from using expired certificate to gain unauthorized access to an Endpoint.</p>
Additional IoT Device Security Capabilities and Practices	System Resiliency	Device must be able to function post security attack (based on no damage. May require SW/FW reinstatement or update)
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	Device must be able to store data and provide access to security breaches during the lifecycle
Additional IoT Device Security Capabilities and Practices	Least Functionality	<p><i>Device should provide mitigation options including device shut-down in the event of a security attack/breach</i></p> <p>a. Network elements must support limited network access for endpoints that do not support 802.1X</p> <p>b. Upon detecting a threat, anNetwork must isolate infected devices based on local policy and report the action to the network administrator.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Physical Access Control	<i>Device should be able to block un-authorized physical access. For direct connection to a device there must be a secure/authorization process</i> Endpoints must protect personally identifiable information from disclosure and modification. The actual implementation will depend on the nature of the endpoint and associated service, but an example would be to encrypt information on board the device such that only authorized users may access it.
Additional IoT Device Security Capabilities and Practices	Best Current Practices	

## 12 | Annex H: Mapping to IoXT Pledge

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	
Secure Device Capabilities - Baseline	Secured Access	<p>[Security Pledge] 1. No universal passwords The product shall not have a universal password; unique security credentials will be required for operation. Products shall either have a unique password or require the user to enter a new password immediately upon first use.</p> <p>[Security Pledge] 2. Secured Interfaces All product interfaces shall be appropriately secured by the manufacturer. In all cases, any external communication interfaces shall be secured. For products in which local attacks are a concern, internal chip-to-chip interfaces may be secured.</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[Security Pledge] 2. Secured Interfaces In all cases, any external communication interfaces shall be secured. All sensitive interfaces shall be encrypted and authenticated.</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[Security Pledge] 3 : Proven cryptography Specifically, suitable cryptographic security techniques and algorithms that are well developed, proven, reviewed and standardized and should be applied wherever possible in place of proprietary developed algorithms, which haven't been subjected to the same level of scrutiny and review.</p>
Secure Device Capabilities - Baseline	Data Validation	<p>[Security Pledge] 5. Signed software updates The product shall only support signed software updates. While it is critical that all products be updatable, it is just as critical that these update images be secured. A manufacturer must cryptographically sign update images to prevent tampering during deployment. The product must not use unsigned updates, as they could be fraudulent.</p> <p>[Security Pledge] 2: Secured Interfaces All sensitive interfaces shall be encrypted and authenticated.</p>
Secure Device Capabilities - Baseline	Event Logging	
Secure Device Capabilities - Baseline	Cryptography	<p>[Security Pledge] 3 : Proven cryptography Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms ioXt Security Pledge participants agree their product's security shall use proven and standardized cryptography. Specifically, suitable cryptographic security techniques and algorithms that are well developed, proven, reviewed and standardized and should be applied wherever possible in place of proprietary developed algorithms, which haven't been subjected to the same level of scrutiny and review.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Patchability	[Security Pledge] 6. Automatically applied updates The manufacturer will act quickly to apply timely security updates. Whenever a security vulnerability is detected, the manufacturer will automatically apply a patch to the product. No user intervention will be required.
Secure Device Capabilities - Baseline	Reprovisioning	
Product Lifecycle Management	Vulnerability Submission and Handling Process	[Security Pledge] 7. Vulnerability reporting program The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.
Product Lifecycle Management	EoL/EoS Updates and Disclosure	[Security Pledge] 8: Security Expiration Date The manufacturer shall be transparent about the period of time that security updates will be provided. Like a manufacturer's product warranty, there shall be transparency around the support period of security updates.
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	[Security Pledge] 2: Secured Interfaces In all cases, any external communication interfaces shall be secured. For products in which local attacks are a concern, internal chip-to-chip interfaces may be secured. Further, memory interface may also be secured through secure boot or other memory integrity checks. All sensitive interfaces shall be encrypted and authenticated.
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	[Security Pledge] 2. Secured Interface For products in which local attacks are a concern, internal chip-to-chip interfaces may be secured. Further, memory interface may also be secured through secure boot or other memory integrity checks.
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	



CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	[Security Pledge] 8. Security expiration date The manufacturer shall be transparent about the period of time that security updates will be provided. Like a manufacturer's product warranty, there shall be transparency around the support period of security updates.
Additional IoT Device Security Capabilities and Practices	Least Functionality	[Security Pledge] 4. Security by default Product security shall be appropriately enabled by default by the manufacturer. This principle guarantees that products are appropriately secured at the time of purchase.
Additional IoT Device Security Capabilities and Practices	Physical Access Control	[Security Pledge] 2. Secured Interface For products in which local attacks are a concern, internal chip-to-chip interfaces may be secured. Further, memory interface may also be secured through secure boot or other memory integrity checks.
Additional IoT Device Security Capabilities and Practices	Best Current Practices	



## 13 | Annex I: Mapping to Open Connectivity Foundation Specifications

The Open Connectivity Foundation (OCF) provides the following mapping of its secure interoperability specification, as of the publication date of this document, to the IoT security capabilities set forth in the above document. OCF continues to revise and expand its specification and associated conformance testing and certification program. To ensure access to the most accurate and up-to-date information on the OCF specification and testing and certification program, please visit <https://openconnectivity.org>.

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 7.1.1.</b> The unique identifier for the device is either sent in the certificate the device sends when establishing communication on the network, or bound to a pre-shared key.
Secure Device Capabilities - Baseline	Secured Access	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clauses: 5,6,7:</b> Prior to operational state, device must be onboarded and configured with either symmetric or asymmetric credentials based on certificates or shared keys Once operational devices implement role-based and/or subject based access control for each resource they present to the network. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12:</b> Access control is enforced over all Resources. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 13.3.1:</b> Stored Credentials used to authenticate server to clients. Note: OCF does not specify physical access controls.
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.2.1:</b> Devices must support TLS/DTLS version 1.2 or greater for all unicast sessions.
Secure Device Capabilities - Baseline	Data At Rest Is Protected	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2:</b> Secure storage for credentials is strongly recommended. [OCF Vendor Attestation Document]: Certification applicant has taken appropriate measures to protect Sensitive Data as defined in OCF Security Specification ISO/IEC 30118-2:2018 Clause 14.2.2
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 5 Figure 3:</b> Shows transport, session and application layer standards. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.2.1:</b> Devices must support CoAP, and CoAP over DTLS. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.3:</b> Cipher Suites: All heavily reviewed and IETF approved or greater.
Secure Device Capabilities - Baseline	Data Validation	<b>[OCF Core Technology Specification ISO/IEC 30118-1:2018].</b> Data model enforcement of encoding, type and length. Data model enforcement occurs on data inbound and outbound to the system. Certification includes schema validation.
Secure Device Capabilities - Baseline	Event Logging	Future work for OCF

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Cryptography	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.3.1:</b> This clause lists the cipher suites allowed during ownership transfer and normal operation. All cipher suites are recognized IETF RFCs and most are IANA supported ciphers. Strong, proven, updateable cryptography using open, peer-reviewed methods and algorithms. NIST approved algorithms for all cryptographic operations.
Secure Device Capabilities - Baseline	Patchability	<b>[OCF Vendor Attestation Document]:</b> Certification Applicant agrees to respond to, address, and patch software vulnerabilities as prescribed by the OCF Security Incident Response Plan. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.3:</b> Process where device validates the software version against a trusted source. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.4:</b> A client with the correct authorization can initiate a software update process.
Secure Device Capabilities - Baseline	Reprovisioning	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 8.2</b> Defines how resources on the device are returned to the manufacturer's default values.
Product Lifecycle Management — Baseline	Vulnerability Submission and Handling Process	<b>[OCF] Security Working Group Incident Response Plan:</b> document addresses reporting (web page dedicated to reporting of issues), mitigation, timeframes, communication, emergency/critical fixes, and software deployment.
Product Lifecycle Management — Baseline	EoL/EoS Updates and Disclosure	<b>[OCF] Updatable Certified Product List:</b> Website. <a href="https://openconnectivity.org/certified-products">https://openconnectivity.org/certified-products</a> manufacturers should notify OCF that device is EoL.
Produce Lifecycle Management - Baseline	Device Intent Documentation	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 9.4.2.2.3 End Entity Certificate Profile:</b> The MUD file pointed to by the URI included in the X.509 certificate includes the following properties referenced in RFC 8520: <b>[RFC 8520] Section 3.7 systeminfo (<a href="https://tools.ietf.org/html/rfc8520#section-3.7">https://tools.ietf.org/html/rfc8520#section-3.7</a>):</b> This is a textual UTF-8 description of the Thing to be connected. The intent is for administrators to be able to see a brief displayable description of the Thing. It SHOULD NOT exceed 60 characters worth of display space. <b>[RFC 8520] Section 4.3 documentation (<a href="https://tools.ietf.org/html/rfc8520#section-4.3">https://tools.ietf.org/html/rfc8520#section-4.3</a>):</b> This URI consists of a URL that points to documentation relating to the device and the MUD file.
Secure Capabilities - Phase In Over Time	Device Intent Signaling	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 9.4.2.2.3 End Entity Certificate Profile:</b> This section details the manner in which devices can signal intent and capabilities beyond those currently in use for security profiles. MUD URI's can be encoded here, as can attestations about meeting differing hardening requirements, certificate trust chains, and more.
Secure Capabilities - Phase In Over Time	Device Network Onboarding	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 3.1.31 Device Configuration Resource (DCR):</b> Includes the WiFi Easy Setup Resources, and the other transport-level onboarding (e.g. Bluetooth) are defined in other specification documents for OCF. <b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 5.3 Onboarding Overview:</b> For non-transport onboarding, the process is specified in great detail as far as establishment of trust, authentication, verification, authorization, local credential issuance, etc.

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4: Additional Security Guidelines and Best Practices:</b> address Software and Secure Development Lifecycle, but OCF is not an application level specification, rather it is a Session-level specification so there will always be additional software added to the foundation OCF provides.
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p><b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.8.3.4: Black Security Profile:</b> requires the manufacturer to install a certificate which chains to the OCF root certificate (which is in each onboarding tool's trust store) to validate the hardware has been OCF Certified by an authorized test lab, that it chains to that manufacturer's intermediate root and that it shares a trust relationship bound to the hardware and secure credential store of the device.</p> <p><b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.2:</b> Hardware Secure storage is recommended for symmetric and asymmetric keys, access credentials and personal private data.</p> <p><b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.7:</b> Defines levels of Hardware Tamper Protection for cryptographic module.</p>
Additional IoT Device Security Capabilities and Practices	Time Distribution	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.5:</b> Secure time source can be external as long as it is signed by a trusted source and the signature validation in the local device is a trusted process (e.g. backed by secure boot).
Additional IoT Device Security Capabilities and Practices	System Resiliency	<b>[OCF]:</b> Certification requires that all devices maintain proximal control in the case of a wide area network outage.
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4-13: Security Hardening Guidelines/ Execution Environment Security:</b> It is recommended that at least one static and dynamic analysis tool be applied to any proposed major production release of the software before its release, and any vulnerabilities resolved.
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	IoTivity is an open source implementation for OCF and lists all software dependencies. <a href="https://iotivity.org/">https://iotivity.org/</a>
Additional IoT Device Security Capabilities and Practices	Least Functionality	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12:</b> Access Control: Employs a deny-all, permit-by-exception policy to allow access to Resources (data and actuators) for Read/Write/Create/Delete/Notify. Access control can be updated dynamically at the location of deployment to limit access (to a role, Device, or implementation).
Additional IoT Device Security Capabilities and Practices	Physical Access Control	<p><b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.7:</b> Defines levels of Hardware Tamper Protection for cryptographic module.</p> <p><b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4:</b> Additional Security Guidelines and Best Practice</p>
Additional IoT Device Security Capabilities and Practices	Best Current Practices	<b>[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4: Additional Security Guidelines and Best Practices:</b> Discuss non-certifiable/non-testable behaviors that are desirable in software development, hardware development, deployment, testing, and hardening areas.

## 14 | Annex J: Mapping to World Wide Web Coalition Web of Things Requirements

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	
Secure Device Capabilities - Baseline	Secured Access	
Secure Device Capabilities - Baseline	Data In Transit Is Protected	
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	
Secure Device Capabilities - Baseline	Data Validation	
Secure Device Capabilities - Baseline	Event Logging	
Secure Device Capabilities - Baseline	Cryptography	See <a href="https://github.com/w3c/wot-security-best-practices">https://github.com/w3c/wot-security-best-practices</a>
Secure Device Capabilities - Baseline	Patchability	
Secure Device Capabilities - Baseline	Reprovisioning	
Product Lifecycle Management	Vulnerability Submission and Handling Process	
Product Lifecycle Management	EoL/EoS Updates and Disclosure	
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	see <a href="https://github.com/w3c/wot-security-testing-plan">https://github.com/w3c/wot-security-testing-plan</a>
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Current Practices	See <a href="https://github.com/w3c/wot-security-best-practice">https://github.com/w3c/wot-security-best-practice</a>



## 15 | Annex K: Mapping to EU Agency for Cybersecurity Baseline Security Recommendations for IoT

This section maps this group's recommendations<sup>34</sup> to the C2 Consensus. Note that the EU Agency for Cybersecurity was previously known as ENISA.

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	[ENISA] (Annex A): GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems, to identify and authenticate of the assets involved in the IoT Service (i.e. Gateways, Endpoint devices, home network, roaming networks, service platforms, etc.).
Secure Device Capabilities - Baseline	Secured Access	<p>[ENISA] (Annex A): GP-TM-09: Establish hard to crack device individual default passwords. Usernames and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked, and a hard to crack default password is still a weakness if it is used for more than one device.</p> <p>[ENISA] (Annex A): GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.</p> <p>[ENISA] (Annex A): GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.</p> <p>[ENISA] (Annex A): GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.</p> <p>[ENISA] (Annex A): GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted</p> <p>[ENISA] (Annex A): GP-TM-25: Protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts, or by making the user wait a certain amount of time to login again after a failed attempt. This protection should also consider keys stored in devices.</p> <p>[ENISA] (Annex A): GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.</p> <p>[ENISA] (Annex A): GP-TM-27: Limit permissions of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users). Implement fine-grained authorisation mechanisms - such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC)- for executing privileged actions, access to files and directories, applications, etc. Use the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.</p> <p>[ENISA] (Annex A): GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[ENISA] (Annex A): GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems, to identify and authenticate of the assets involved in the IoT Service (i.e. Gateways, Endpoint devices, home network, roaming networks, service platforms, etc.).</p> <p>[ENISA] (Annex A): GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.</p> <p>[ENISA] (Annex A): GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.</p> <p>[ENISA] (Annex A): GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.</p> <p>[ENISA] (Annex A): GP-TM-40: Ensure credentials are not exposed in internal or external network traffic</p> <p>[ENISA] (Annex A): GP-TM-41: Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.</p> <p>[ENISA] (Annex A): GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the end point is diverted to a remediation network for action.</p> <p>[ENISA] (Annex A): GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[ENISA] (Annex A): GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.</p>
Secure Device Capabilities - Baseline	Data Validation	<p>[ENISA] 4.3.13 Secure input and output handling</p> <p>GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Event Logging	[ENISA] (Annex A): GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection.
Secure Device Capabilities - Baseline	Cryptography	<p>[ENISA] (Annex A): GP-TM-35: Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance.</p> <p>[ENISA] (Annex A): GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques (including entities secure identification, secure configuration, etc.) that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable so to minimise the management effort and maximise their usability.</p> <p>[ENISA] (Annex A): GP-TM-37: Support scalable key management schemes. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection.</p>
Secure Device Capabilities - Baseline	Patchability	<p>[ENISA] (Annex A): GP-TM-18: Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.</p> <p>[ENISA] (Annex A): GP-TM-19: Offer an automatic firmware update mechanism. Devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default. A device may offer an option to disable automatic firmware updates and require authentication for it.</p> <p>[ENISA] (Annex A): GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not change network protocol interfaces in any way that is incompatible with previous versions. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Users should have the ability to approve, authorise or reject updates.</p>
Secure Device Capabilities - Baseline	Reprovisioning	<p>[ENISA] (Annex A): GP-OP-01: Develop an end-of-life strategy for IoT products. Security patches and updates will eventually be discontinued for some IoT devices. Therefore, developers should prepare and communicate a product sunset plan from the initial stages to ensure that manufacturers and consumers are aware of the risks posed to a device beyond its expected expiry date.</p> <p>[ENISA] (Annex A): GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Product Lifecycle Management	Vulnerability Submission and Handling Process	<p>[ENISA] (Annex A): GP-OP-03: Monitor the performance and patch known vulnerabilities up until the “end-of-support” period of a product’s lifecycle. Due to the limited life cycle of many IoT devices, critical, publicly known security or privacy bugs will pose a risk to consumers using outdated devices.</p> <p>[ENISA] (Annex A): GP-OP-05: Establish procedures for analysing and handling security incidents. For any incident there should be a response to:</p> <ol style="list-style-type: none"> <li>confirm the nature and extent of the incident;</li> <li>take control of the situation;</li> <li>contain the incident; and</li> <li>communicate with stakeholders</li> </ol> <p>Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents.</p> <p>ENISA] (Annex A): GP-OP-06: Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).</p> <p>ENISA] (Annex A): GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.</p> <p>ENISA] (Annex A): GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies’ own internal security teams may not catch.</p>
Product Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p>[ENISA] (Annex A): GP-TM-01: Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.</p> <p>[ENISA] (Annex A): GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device — for example, specialised security chips/ coprocessors that integrate security at the transistor level, embedded in the processor, that provide: (see [ENISA] document for full list)</p>





CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Current Practices	



## 16 | Annex L: Mapping to ETSI 103 645

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	
Secure Device Capabilities - Baseline	Secured Access	<p>[ETSI] 4.1: No universal default passwords</p> <p>[ETSI] Provision 4.1-1 All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.</p> <p>[ETSI] Provision 4.6-1 Unused software and network ports should be closed.</p> <p>[ETSI] Provision 4.6-2 Hardware should not unnecessarily expose access to attack (e.g. open serial access, ports or test points).</p> <p>[ETSI] Provision 4.6-3 Software services should not be available if they are not used.</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[ETSI] 4.4 Securely store credentials and security-sensitive data</p> <p>[ETSI] 4.5 Communicate securely</p> <p>[ETSI] Provision 4.5-1 Security-sensitive data, including any remote management and control, should be encrypted in transit, with such encryption appropriate to the properties of the technology and usage.</p> <p>[ETSI] Provision 4.5-2 All keys should be managed securely.</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	<p>[ETSI] Provision 4.10-1 If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.</p> <p>[ETSI] Provision 4.10-2 If telemetry data is collected from IoT devices and services, the processing of personal data should be kept to a minimum and such data should be anonymized.</p> <p>[ETSI] Provision 4.10-3 If telemetry data is collected from IoT devices and services, consumers shall be provided with information on what telemetry data is collected and the reasons for this.</p>
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[ETSI] 4.5 Communicate securely</p> <p>The use of open, peer-reviewed standards is strongly encouraged.</p>
Secure Device Capabilities - Baseline	Data Validation	<p>[ETSI] Provision 4.13-1 Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.</p>
Secure Device Capabilities - Baseline	Event Logging	<p>[ETSI] Provision 4.7-2 If an unauthorized change is detected to the software, the device should alert the consumer and/or administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.</p>
Secure Device Capabilities - Baseline	Cryptography	

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Patchability	<p>[ETSI] 4.3 Keep software updated</p> <p>Provision 4.3-1 All software components in consumer IoT devices should be securely updateable.</p> <p>Provision 4.3-2 The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required.</p> <p>Provision 4.3-3 When software components are updateable, updates shall be timely.</p> <p>Provision 4.3-4 When software components are updateable, an end-of-life policy shall be published for devices that explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. This policy shall be published in an accessible way that is clear and transparent to the consumer.</p> <p>Provision 4.3-5 When software components are updateable, the need for each update should be made clear to consumers and an update should be easy to implement.</p> <p>Provision 4.3-6 When software components are updateable, updates should, where possible, maintain the basic functioning of the device, which can be critical to remain available during an update.</p> <p>Provision 4.3-7 When software components are updateable, the provenance of software updates should be assured and security patches should be delivered over a secure channel.</p> <p>Provision 4.3-8 For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.</p> <p>Provision 4.3-9 For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period of hardware replacement support and an end-of-life policy should be published in an accessible way that is clear and transparent to the consumer.</p>
Secure Device Capabilities - Baseline	Reprovisioning	
Product Lifecycle Management	Vulnerability Submission and Handling Process	<p>[ETSI] 4.2: Implement a means to manage reports of vulnerabilities</p> <p>Provision 4.2-1: Companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.</p> <p>Provision 4.2-2 Disclosed vulnerabilities should be acted on in a timely manner.</p> <p>Provision 4.2-3 Companies should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate as part of the product security lifecycle.</p>
Product Lifecycle Management	EoL/EoS Updates and Disclosure	
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Capabilities - Phase In Over Time	Device Network Onboarding	[ETSI] 4.12 Make installation and maintenance of devices easy [ETSI] Provision 4.12-1 Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	Provision 4.7-1 Software on IoT devices should be verified using secure boot mechanisms, which require a hardware root of trust.
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	[ETSI] Provision 4.9-1 Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. [ETSI] Provision 4.9-2 As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. [ETSI] Provision 4.9-3 Devices should be able to return to a network in an expected, operational and stable state and in an orderly fashion, rather than in a massive-scale reconnect.
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	[ETSI] Provision 4.6-4 Code should be minimized to the functionality necessary for the service/device to operate. [ETSI] Provision 4.6-5 Software should run with least necessary privileges, taking account of both security and functionality.
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Current Practices	

## 17 | Annex M: Mapping to GSMA IoT Security Guidelines for Endpoint Ecosystems

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	
Secure Device Capabilities - Baseline	Secured Access	<p>[GSMA] 6.9 Endpoint Password Management</p> <p>Devices that incorporate user interfaces must be capable of managing passwords effectively. This requires several things</p> <ul style="list-style-type: none"> <li>• Brute-force attack mitigation</li> <li>• Disabling the use of default or hardcoded passwords</li> <li>• Password best-practice enforcement</li> <li>• Disallowing display of user credentials on login interfaces</li> <li>• Enforcing thresholds and incremental delays for invalid password attempts</li> </ul> <p>[GSMA] 6.12 Remote Endpoint Administration</p> <p>While not all Endpoints require remote administration, the ones that do must be architected in a way that ensures that third parties cannot abuse administrative credentials to compromise some (or all) of the Endpoints in the field. The appropriate solution will depend on the capabilities of the Endpoint</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[GSMA] 6.14 Enforce Memory Protection</p> <p>Embedded systems are often designed with microcontrollers that are not capable of robust technology such as Memory Management Units (MMU) and Memory Protection Units (MPU)... implement memory protection with either an MPU or MMU.</p> <p>[GSMA] 6.15 Bootloading Outside of Internal ROM</p> <p>Consider using a CPU or MCU/MPU with an internal ROM or lock-capable NVRAM to store the bootloader. This will help to ensure that the platform can at least verify the first executable loaded and executed by the architecture, resulting in a more trustworthy device.</p> <p>[GSMA] 6.16 Locking Critical Sections of Memory</p> <p>Critical applications stored in executable regions of memory, such as first-stage bootloaders or Trusted Computing Bases, should be stored read-only</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[GSMA] 6.19 Endpoint Communications Security</p> <p>This process is made far simpler through the use of existing and well analysed security protocols, such as, but not limited to:</p> <ul style="list-style-type: none"> <li>• The latest approved TLS standard</li> <li>• The latest approved DTLS standard</li> <li>• SSH2 for authentication and key exchange</li> <li>• GBA for key generation and exchange</li> <li>• OAuth2 for authorization</li> </ul>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Data Validation	
Secure Device Capabilities - Baseline	Event Logging	<p>[GSMA] 6.13 Logging and Diagnostics</p> <p>In order to assess problems with Endpoint devices, the IoT Service Provider should constantly evaluate the behaviour of the Endpoint and determine whether the Endpoint is functioning within the set of approved behaviours. To accomplish this, three strategies should be used</p> <ul style="list-style-type: none"> <li>• Anomaly detection</li> <li>• Endpoint logging</li> <li>• Endpoint diagnostics</li> </ul>
Secure Device Capabilities - Baseline	Cryptography	
Secure Device Capabilities - Baseline	Patchability	
Secure Device Capabilities - Baseline	Reprovisioning	
Product Lifecycle Management	Vulnerability Submission and Handling Process	
Product Lifecycle Management	EoL/EoS Updates and Disclosure	
Product Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	<p>[GSMA] 6.8 Uniquely Provision Each Endpoint</p> <p>While personalization guarantees that each device is unique once it is manufactured, provisioning ensures that a unique device is activated, updated, and associated with a particular customer identity. The provisioning process helps separate devices that have been manufactured from devices that have been purchased and/or deployed in an IoT environment.</p> <p>[GSMA] 6.20 Authenticating an Endpoint Identity</p> <p>If each Endpoint carries a cryptographically unique identity, such as a unique serial number, the device must be able to prove that it truly represents that serial number.</p>
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	





CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p>[GSMA] 6.1 Implement an Endpoint Trusted Computing Base</p> <p>The first step in securing any embedded system is the definition of the Trusted Computing Base (TCB). In the context of an Endpoint (or similar embedded devices), a TCB is a suite composed of hardware, software, and protocols that ensures the integrity of the Endpoint, performs mutual authentication with network peers, and manages communications and application security.</p> <p>[GSMA] 6.2 Utilize a Trust Anchor</p> <p>In order for an Endpoint to participate in an ecosystem, it must be able to verify the integrity of its own platform, and must be able to authenticate the identity of its peers. To do this, Endpoints require a trust anchor incorporated into a Trusted Computing Base.</p> <p>A trust anchor is a secure hardware element, either a separate physical chip, or a secure core inside a CPU, that is capable of securely storing and processing cryptographic secrets. A UICC or eUICC device is an example of a secure technology that can be used as a trust element to store authentication secrets.</p> <p>[GSMA] 6.3 Use a Tamper Resistant Trust Anchor</p> <p>[GSMA] 6.4 Define an API for Using the TCB</p> <p>[GSMA] 6.5 Defining an Organizational Root of Trust</p> <p>[GSMA] 6.6 Personalize Each Endpoint Device Prior to Fulfilment</p> <p>[GSMA] 6.7 Minimum Viable execution Platform (Application Roll-Back)</p>
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	
Additional IoT Device Security Capabilities and Practices	Least Functionality	
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Current Practices	

## 18 | Annex N: Mapping to Draft NISTIR 8259

As of this writing, NISTIR 8259 is released in draft form for public comment. The mapping below shows likely places to explore the commonalities between the C2 Consensus baseline and the NIST Core Baseline in 8259, including sample text illustrating the general direction taken in 8259. A link to the full NISTIR 8259 draft is shown in Annex D: Informative References.

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	[NISTIR 8259] Table 1 row 1, Device Identification: The IoT device can be uniquely identified logically and physically.
Secure Device Capabilities - Baseline	Secured Access	[NISTIR 8259] Table 1 row 2, Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only. Table 1 row 4, Logical Access to Interfaces: The IoT device can limit logical access to its local and network interfaces to authorized entities only.
Secure Device Capabilities - Baseline	Data In Transit Is Protected	[NISTIR 8259] Table 1 row 3, Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Secure Device Capabilities - Baseline	Data At Rest Is Protected	[NISTIR 8259] Table 1 row 3, Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	
Secure Device Capabilities - Baseline	Data Validation	
Secure Device Capabilities - Baseline	Event Logging	[NISTIR 8259] Table 1 row 6, Cybersecurity Event Logging: The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.
Secure Device Capabilities - Baseline	Cryptography	[NISTIR 8259] Table 1 row 3, Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Secure Device Capabilities - Baseline	Patchability	[NISTIR 8259] Table 1 row 5, Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
Secure Device Capabilities - Baseline	Reprovisioning	[NISTIR 8259] Table 1 row 2, Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only. Table 1 row 4, Logical Access to Interfaces: The IoT device can limit logical access to its local and network interfaces to authorized entities only.

CATEGORY	SUB-CATEGORY	MAPS TO
Product Lifecycle Management	Vulnerability Submission and Handling Process	<p>[NISTIR 8259] Section 7: Manufacturers accepting and responding to vulnerability reports helps customers maintain the cybersecurity of their IoT devices as new threats emerge. SSDF practices:</p> <ul style="list-style-type: none"> <li>• RV.1, Identify and Confirm Vulnerabilities on an Ongoing Basis</li> <li>• RV.2, Assess and Prioritize the Remediation of All Vulnerabilities</li> <li>• RV.3, Analyze Vulnerabilities to Identify Their Root Causes</li> </ul>
Product Lifecycle Management	EoL/EoS Updates and Disclosure	[NISTIR 8259] Section 6: Support and Lifespan Expectations
Produce Lifecycle Management	Device Intent Documentation	[NISTIR 8259] Section 6: Sufficient information on the IoT device's operational characteristics so they can adequately secure the device (e.g., make information on characteristics available on a website...).
Secure Capabilities - Phase In Over Time	Device Intent Signaling	[NISTIR 8259] Section 6: Sufficient information on the IoT device's operational characteristics so they can adequately secure the device (e.g., ...use a standard protocol so devices can provide basic information to authorized parties).
Secure Capabilities - Phase In Over Time	Device Network Onboarding	
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	Section 7, Secure Development Practices for IoT Devices
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	Section 5.1, Device Specifications: Use hardware-based cybersecurity features. An example is having a hardware root of trust that provides trusted storage for cryptographic keys and enables performing secure boots and confirming device authenticity.
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	[NISTIR 8259] Section 6: Cybersecurity Information to Provide to Customers
Additional IoT Device Security Capabilities and Practices	Least Functionality	[NISTIR 8259] Section 3.2, Device Cybersecurity Features: Do not include unneeded features provided by hardware, firmware, and/or the operating system; if the inclusion of such features cannot be avoided, ensure they can be disabled to prevent misuse and exploitation.

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Physical Access Control	[NISTIR 8259] Section 3.2, Device Cybersecurity Features: ...if a device has local interfaces on its external housing and the device is likely to be deployed in public areas, possible approaches include offering a tamper-resistant enclosure to prevent physical access to the interfaces, and offering a configuration option that logically disables the interfaces.
Additional IoT Device Security Capabilities and Practices	Best Current Practices	

## 19 | Annex O: Mapping to UK DCMS Code of Practice for Consumer IoT Security

<https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	
Secure Device Capabilities - Baseline	Secured Access	[DCMS] 1. No default passwords All IoT device passwords shall be unique and not resettable to any universal factory default value
Secure Device Capabilities - Baseline	Data In Transit Is Protected	[DCMS] 4. Securely store credentials and security-sensitive data Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable. [DCMS] 5. Communicate securely Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.
Secure Device Capabilities - Baseline	Data At Rest Is Protected	
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	
Secure Device Capabilities - Baseline	Data Validation	[DCMS] 13. Validate input data Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.
Secure Device Capabilities - Baseline	Event Logging	
Secure Device Capabilities - Baseline	Cryptography	
Secure Device Capabilities - Baseline	Patchability	[DCMS] 3. Keep software updated Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.



CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Reprovisioning	[DCMS] 11. Make it easy for consumers to delete personal data.
Product Lifecycle Management	Vulnerability Submission and Handling Process	[DCMS] 2. Implement a vulnerability disclosure policy All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.
Product Lifecycle Management	EoL/EoS Updates and Disclosure	
Product Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	
Secure Capabilities - Phase In Over Time	Device Network Onboarding	[DCMS] 12. Make installation and maintenance of devices easy
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	7. Ensure software integrity (Software on IoT devices should be verified using secure boot mechanisms....)
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	[DCMS] 9. Make systems resilient to outages Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	



CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Least Functionality	[DCMS] 6. Minimise exposed attack surfaces All devices and services should operate on the ‘principle of least privilege’; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.
Additional IoT Device Security Capabilities and Practices	Physical Access Control	
Additional IoT Device Security Capabilities and Practices	Best Practices	

## 20 | Annex P: Mapping to UL MCV 1376 — Security Capabilities Verified

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Device Identifiers	None.
Secure Device Capabilities - Baseline	Secured Access	<p>[UL] 2.1 System defaults such as password, certificates, and/or cryptographic keys must be changed on initial setup</p> <p>Ideally, system defaults should be avoided — but realistically that’s not always possible. It may be necessary for something to be set to a default value to allow for the ‘boot-strapping’ of the system for the first time. However, the risk of using the default should be clearly outlined to the people operating that system for that first time, and this requirement outlines the need to force them to make a change from this default as part of the overall setup.</p> <p>[UL] 2.2 Password Policy</p> <p>Passwords are often required and implemented to provide authentication of users. If not set to a value that is sufficiently secure, they can be easily guessed or brute-forced to bypass this authentication, allowing a bad-actor to gain access to the services the passwords are supposed to protect. Many attacks on devices are based on exploiting insecure, or default, password values.</p> <p>Minimum levels for password security to sensitive services must be enforced, such that there is less than a 1 in 100,000 chance that any guess will be correct and that attempts to brute force the password domain in the device cannot be performed in less than 24 hours. These protections may include combinations of password strength and ‘back off’ timers on any password entry mechanisms to slow entry during high volume password entry attempts. System designers should consider the needs of customers to re-enter incorrect passwords cause through typographic errors, along with the need (or lack thereof) to support many hundreds or thousands of password entry attempts within a relatively short (e.g., 24 hour) period.</p> <p>[UL] 2.3 Sensitive data must be protected against exposure and unauthenticated modification</p> <p>Bad-actors will often attempt to recover sensitive data, such as passwords, secret cryptographic keys, and customer data, as the start of an attack on a system. This data may be easily accessed if it is not protected, and electronic protection must always involve strong cryptography and key management to ensure that it is providing the controls at a sufficient level. Therefore any data that is communicated across connections that are not physically direct (such as a direct USB or serial connection) must be protected against disclosure through cryptographic means.</p> <p>[UL] 3.1 Communication and debug ports must be protected against misuse</p> <p>Often devices will come with some interfaces that are either specifically designed, or can be used, for ‘debugging’ purposes. Additionally, all devices must of course have methods for communication. Such ports may be external or internal, allow for remote or local-only access, but all must be secured to prevent exploit. For example, local ‘JTAG’ ports can often be used to extract software from devices and start the reverse engineering process which allows for determination of vulnerabilities within the device. Alternatively, a device may have remote communications — such as Wi-Fi, Ethernet, or others — which allows for data to be routed into and out of the device.</p> <p>Access to such ports therefore needs not be physical, but they may contain vulnerabilities or weaknesses that can be exploited to bypass protections in the device, expose customer PII, or install malware.</p> <p><i>(continued next page)</i></p>

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Secured Access	<p>The vendor must maintain a comprehensive list of all interfaces that the device supports — both physical and logical/protocol. This list must outline what access is provided across each of these interfaces, and how misuse of these interfaces and features is prevented through the design and implementation of the system.</p> <p>[UL] 4.1 Sensitive services must require authentication and ensure the confidentiality and integrity of data</p> <p>Sensitive services within a device are considered to be services which allow for the allocation or changing of security settings, or which allow for access to customer personal information (such as authentication data, email addresses, etc.). Such access is inherently security sensitive, and therefore requires authentication to be performed to ensure that any changes are being correctly performed by the customer, and are not being accessed or altered by a bad-actor. This includes ensuring that access, once authenticated, ensures the integrity of data as it is passed into the device, as well as ensuring confidentiality of any customer data during transport.</p>
Secure Device Capabilities - Baseline	Data In Transit Is Protected	<p>[UL] [UL] 2.4 Industry standard cryptographic algorithms must be used for security services</p> <p>Cryptography has advanced to a point where there are common, standardized algorithms which are known to provide strong protection of data when correctly implemented. Development of proprietary, or bespoke, algorithms or protections actually weakens systems as such algorithms will not have undergone the many years of academic review and attack that is performed on those industry standard methods. Therefore, protections can only be assumed when such standard algorithms are used.</p>
Secure Device Capabilities - Baseline	Data At Rest Is Protected	<p>[UL] 2.3 Sensitive data must be protected against exposure and unauthenticated modification</p> <p>Bad-actors will often attempt to recover sensitive data, such as passwords, secret cryptographic keys, and customer data, as the start of an attack on a system. This data may be easily accessed if it is not protected, and electronic protection must always involve strong cryptography and key management to ensure that it is providing the controls at a sufficient level. Therefore any data that is communicated across connections that are not physically direct (such as a direct USB or serial connection) must be protected against disclosure through cryptographic means.</p> <p>Additionally, storage of such sensitive data must also be protected as customers are likely to re-use passwords across different devices, or even re-purpose online passwords for home use. This includes ensuring that such data is not easily accessible with internal access to the device (eg through monitoring an internal serial bus). It is understood that sometimes such data must be displayed for business and user interface reasons (e.g. to display and receive a user password as it is entered), but business justification for each exposure must be provided.</p> <p>It is best practice to use a single ‘housekeeping’ key that is used as a master key for storage and protection of other sensitive data. Of course, this single key must then be stored securely, but it ensures that other data encrypted with this key can be maintained with lesser security, and may be transmitted across external busses without risk. The datagram format for the encryption of this data should accommodate for the type of data being encrypted — for example so that a simple password encrypted under the housekeeping key cannot be substituted for a more complex cryptographic key.</p> <p>Housekeeping keys must be stored securely, and never exposed in external memory or busses. It is a later requirement that the software which has the privilege to access this housekeeping key is executed at a more secure privilege to any code that has access to external ports or interfaces. Such keys must also be unique per device, as per the requirements of A.2.1.</p>



CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	<p>[UL] 6.5 Switched or wireless connections must allow for the use of an industry standard security protocol (such as TLS)</p> <p>A formal security protocol is essential when communicating over remote or wireless connections. It is a requirement that systems allow for the use of an industry standard ‘best practice’ public protocol (such as TLS). A proprietary protocol that has been designed with the light weight needs of the IoT space in mind may also be implemented, but customers must be provided with the ability to choose which protocol they wish to use, and any proprietary protocols implemented may require the device to undergo more detailed testing. It should be noted that this requirement does not mandate that all communications must be performed using this protocol — for example, a light bulb may allow for the changing of brightness without implementing encryption of the command — but the protocol must be available for use, and must always be used for any security sensitive communications.</p>
Secure Device Capabilities - Baseline	Data Validation	<p>[UL] 4.4 No direct execution of scripts/commands</p> <p>Functionality that allows for the direct execution of scripts or commands by the device or system can often be exploited by a malicious party. Such functionality should not be natively supported, and any methods for the customer to supply executable code or scripts must be parsed and sanitized to ensure that it does not expose weaknesses or allow for the exploitation of security vulnerabilities in the system.</p>
Secure Device Capabilities - Baseline	Event Logging	<p>[UL] 3.8 Logging and error messages must not expose sensitive data without authentication</p> <p>It is often necessary for systems to be placed into a ‘debug’ or ‘logging’ mode to facilitate the identification and remediation of problems with the device. However, such data may be used to gain information about the system, or to obtain data that should otherwise remain confidential. Therefore, it is important that any functions that allow for the logging of sensitive data are disabled by default and can only be temporarily enabled after suitable authentication. Once enabled, such logging should not remain active for more than 15 minutes, to ensure that the logging state is not accidentally left active.</p> <p>It is also strongly recommended that any sensitive data that is logged is secured with cryptography (eg through encryption using a public key on the device). Any upload or exfiltration of customer identifiable data from the customer premises in such logs must be covered under the privacy policy of the system, and require an opt-in from the customer to accept the transfer of this data.</p> <p>Error messages may also result in the exposure of information — for example, detailing an error with the padding in a cryptographic message can sometimes help attackers determine the values of sensitive information. Therefore, error messages must be carefully designed to not expose details that are too specific about the error state, and instead simply inform the user that an error has occurred. Timing of error messages must also be carefully managed; for example, common compare functions will return an error as quickly as they can, and therefore if used in comparison functions on sensitive data (eg passwords) could accidentally expose information about how many characters of the sensitive data are in fact the same. For this reason, non-timing dependent compare functions are recommended for use with sensitive information, and passwords must not be compared directly with stored plaintext (instead comparing against a hashed value, such as that calculated through the BCrypt function).</p>
Secure Device Capabilities - Baseline	Cryptography	<p>[UL] 2.4 Industry standard cryptographic algorithms must be used for security services</p> <p>Cryptography has advanced to a point where there are common, standardized algorithms which are known to provide strong protection of data when correctly implemented. Development of proprietary, or bespoke, algorithms or protections actually weakens systems as such algorithms will not have undergone the many years of academic review and attack that is performed on those industry standard methods. Therefore, protections can only be assumed when such standard algorithms are used.</p>



CATEGORY	SUB-CATEGORY	MAPS TO
Secure Device Capabilities - Baseline	Patchability	<p>[UL] 1.1 Software updates must be supported, using network or wireless interfaces where available</p> <p>No matter how well software is designed or tested, there will always be bugs and vulnerabilities that are missed. This is just a fact of software development and the sheer complexity of any body of code. So, the update of the software must be allowed in any device to ensure that it can be patched when any such bugs are found. It is an additional requirement that the software update must be able to be performed across a wireless or network interface, should the device provide such an interface. This increases the ease of use for the customer, removing disincentives to install updates.</p> <p>[UL] 1.3 Software updates must be cryptographically authenticated, and provide anti-roll back features</p> <p>Although it is important to support software updates to ensure that devices can be patched and maintained in the field, such features can lead to additional vulnerabilities — where a ‘bad actor’ can install their own software into the device to prevent its normal operation.</p> <p>To prevent this, it’s important that any software update is cryptographically authenticated. Often this will be implemented by using a digital signature across the firmware image, which can be checked by the original firmware (or bootloader of the device) prior to installation. Using a digital signature based on a public key algorithm (such as RSA, or DSA) ensures that the devices themselves don’t need the part of the key (the private or secret key) that is used to generate the authentication data.</p> <p>Where a symmetric key system — such as a (H)MAC — is used, the secret key in each device must be unique per device. Otherwise once the firmware of one device is exposed (eg through a physical attack on that one device), a valid firmware signature for all other devices of this type can be created. Therefore, public key cryptography is recommended to avoid the complexities of managing unique symmetric keys across device portfolios.</p> <p>It is additionally required that the update implements ‘anti-rollback’ features — such as a ‘monotonic’ version number which is included in each release (that is a version number that only increases with each version), which is also checked to ensure that any bad actor can’t just install a previous version of firmware; to ‘reinstate’ any otherwise patched vulnerabilities.</p>
Secure Device Capabilities - Baseline	Reprovisioning	<p>[UL] 4.2 Permanent erasure of sensitive data must be supported</p> <p>Devices must protect sensitive data even during decommissioning (e.g. to prevent the exposure of customer Wi-Fi passwords after disposal or resale), and therefore implement either a ‘factory reset’ which permanently erases all data and configuration from the device, or provide strong protections to the data even given unrestricted physical access to the device. Where the device supports a network interface, it must be possible to ‘remotely decommission’ the device. At all times, a local decommission procedure must always be provided — this may be passive; e.g. erasure of RAM storage after disconnection from power, but where passive mechanisms are implemented they must operate within less than 8 hours and be shown to ensure permanent erasure.</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Product Lifecycle Management	Vulnerability Submission and Handling Process	<p>[UL] 7.2 A vulnerability management and disclosure program must be maintained</p> <p>It has been noted above that it is impossible to find all bugs and vulnerabilities in software, and therefore it can be expected that new issues will become apparent in systems after evaluation and shipping to the customer. Therefore, it is necessary for system vendors to ensure that they have a vulnerability management and disclosure program to maintain the security of their products once shipped. This program must include processes for:</p> <ul style="list-style-type: none"> <li>• Monitoring for new vulnerabilities in all code that it contained in the software composition list</li> <li>• Testing if vulnerabilities affect the vendor systems, and how they can be mitigated if the system is affected</li> <li>• The creation and testing of a patch for the vulnerability if required</li> <li>• Informing customers of the potential vulnerability, and any mitigating steps they can take whilst a patch is being created</li> </ul> <p>[UL] 7.1 A documented process for the distribution of patches/updates must be maintained</p> <p>The final step to fixing a known vulnerability is to issue the patch to the customer/device. This must follow a clear process — which need not be complex, but must clearly outline the steps involved in approving, signing, and distributing the new code.</p> <p>This is required because it is often when there is a ‘rush’ to fix a problem that important security steps are missed, resulting in an even worse situation and more potential exposure of the systems which were being patched.</p>
Product Lifecycle Management	EoL/EoS Updates and Disclosure	<p>[UL] 7.2 A vulnerability management and disclosure program must be maintained</p> <p>It has been noted above that it is impossible to find all bugs and vulnerabilities in software, and therefore it can be expected that new issues will become apparent in systems after evaluation and shipping to the customer. Therefore, it is necessary for system vendors to ensure that they have a vulnerability management and disclosure program to maintain the security of their products once shipped. This program must include processes for:</p> <ul style="list-style-type: none"> <li>• Monitoring for new vulnerabilities in all code that it contained in the software composition list</li> <li>• Testing if vulnerabilities affect the vendor systems, and how they can be mitigated if the system is affected</li> <li>• The creation and testing of a patch for the vulnerability if required</li> <li>• Informing customers of the potential vulnerability, and any mitigating steps they can take whilst a patch is being created</li> </ul> <p>[UL] 7.1 A documented process for the distribution of patches/updates must be maintained</p> <p>The final step to fixing a known vulnerability is to issue the patch to the customer/device. This must follow a clear process — which need not be complex, but must clearly outline the steps involved in approving, signing, and distributing the new code.</p> <p>This is required because it is often when there is a ‘rush’ to fix a problem that important security steps are missed, resulting in an even worse situation and more potential exposure of the systems which were being patched</p>
Produce Lifecycle Management	Device Intent Documentation	
Secure Capabilities - Phase In Over Time	Device Intent Signaling	

CATEGORY	SUB-CATEGORY	MAPS TO
Secure Capabilities-Phase In Over Time	Device Network Onboarding	<p>[UL] 6.3 Connections to remote services must implement cryptographic authentication</p> <p>Remote access connections are especially vulnerable to attack and misuse, and so require special attention when it comes to security. Many interfaces are expected to use TLS for security, but TLS in and of itself is often not sufficient — so it is necessary not only to ensure the correct configuration of those protocols, but also that the authentication channel is ensuring that the customer can authenticate the server. This often requires validation of the complete TLS certificate, including organization, name and other fields, so that the interface cannot be intercepted and manipulated by a bad-actor who has their own TLS certificate. Other protocols may be similarly vulnerable, and would require other controls</p>
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	<p>[UL] 3.5 System software should be free of publically disclosed vulnerabilities</p> <p>It is increasingly common for systems to be composed of various types and sources of software — from internally developed, to externally developed open source or commercial software. For any externally developed software component, it is possible — and indeed likely — that there are previously disclosed vulnerabilities which have been patched and/or mitigated in further updates to the software. Therefore, it is an essential part of securing software to first identify what externally developed software components exist, and using this list to confirm that these components are up to date and sufficiently mitigate any previously identified vulnerabilities.</p> <p>It should be noted that — although it is desirable — it is not an absolute requirement that the very latest version is always used if existing vulnerabilities have been mitigated in other ways.</p> <p>[UL] 3.7 System software must be tested to check for undisclosed vulnerabilities</p> <p>Although much software may be re-used from other sources, it is unlikely that a device will contain absolutely no internally developed code. In addition, the combination of different software components can open up new threat vectors and potential vulnerabilities. Therefore, it is important that some checking is performed against the software of a device in an attempt to identify such vulnerabilities. The intent of this testing is not to perform an exhaustive penetration test against all features and code of the device, as this would be expensive in terms of both time and direct costs — but to confirm that simple attacks are not possible on the system.</p>
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	<p>[UL] 1.5 Device implements a hardware based root of trust for updates and boot authentication</p> <p>Although authenticating software updates is one important aspect of security, ensuring that any code is authenticated upon each boot of the device is also important. This ensures that even if changes are made to the executing code through some exploit, the changes cannot be made permanent and a reboot can be ensured to remove the malicious code.</p>
Additional IoT Device Security Capabilities and Practices	Time Distribution	
Additional IoT Device Security Capabilities and Practices	System Resiliency	<p>[UL] 4.3 Manual backup/override must be provided for safety related services</p> <p>Safety related services, such as those performed by door locks, are increasingly being automated and enabled through digital systems. This requirement outlines the need of such systems to provide is a safety mechanism that ensures any failure of the device — either through malware, lack of power, or coding flaw — does not result in a safety issue that could lead to risk of life. For example, door locks should provide a manual method for locking and unlocking (such as a ‘standard’ key).</p>

CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	<p>[UL] 3.4 Memory and compiler protections must be implemented</p> <p>Modern processing systems and compilers provide multiple methods to assist in the exploitation of any vulnerabilities which may exist in the source code of the device. By correctly enabling and implementing such protections, the security posture of the system can be greatly increased. This requirement does not seek to mandate which protections should be implemented, as this will depend on the specific processing system/operating system/and compiler used — for example, Address Space Layout Randomisation may be implemented in many modern, complex operating systems, but is often not used in smaller Real Time Operating Systems which can have other protection methods. However, it is essential that the vendor demonstrate an understanding of the protections that are available and justify the use (or lack of use) of the protections that they have chosen to implement.</p>
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	<p>[UL] 7.4 A ‘Software Composition List’ must be maintained</p> <p>It is an unfortunate truism that all software contains bugs. It is not possible for any amount of testing to find, and allow for the remediation of, all bugs in any reasonably sized body of code — which is why on-going maintenance of such code is so important. However, it is increasingly common today for the software in a device to be created from various ‘software components’ — open source code, third party libraries, and external binary files. Therefore, in order to maintain code it is not sufficient to simply maintain the code that has been created directly by the product vendor; it is necessary to ensure that all additional ‘software components’ are maintained and updated as well.</p> <p>To achieve this, it is necessary to create and keep up to date a ‘software composition list’ (sometimes called a ‘software bill of materials’) which indicates all of the different software components used in a particular build, as well as their versions. This list must be exhaustive; think of it as an ingredient list for your software, if all of the ingredients are not listed, the recipe will not turn out correctly. In this instance, if not all software is listed, you will not be able to securely maintain your device.</p> <p>Using this composition list, in concert with the vulnerability management program required below, it is possible to ensure that when there is a new vulnerability found in some third party or open source code that is used in the device, it can be noted, investigated, and where necessary patched.</p>
Additional IoT Device Security Capabilities and Practices	Least Functionality	<p>[UL] 3.9 Systems must implement ‘least privilege’, or utilize hardware based features to protect sensitive code and data</p> <p>All software has vulnerabilities, and it is essential that ‘defense in depth’ measures are used to protect against the successful exploit of any newly discovered flaws. This leads to the implementation of ‘least privilege’ in systems, where software is assigned only the execution privilege and access rights that are sufficient and absolutely essential for its required operation. Modern processing and operating systems provide many different methods for this to be achieved, and this requirement is not intended to mandate a specific implementation, but instead ensure that the device vendor has considered what access rights are necessary and put in place measures to ensure that additional access is prevented, or at least mitigated. For example, ‘sandboxing’ or virtualized environments may be used, or access between assets and functions may be managed through assigning lower processor and/or operating system privilege levels to all code that does not require full access to the hardware of the device.</p> <p><i>(continued next page)</i></p>





CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Least Functionality	<p>[UL] 3.6 Unwanted/unnecessary features are removed</p> <p>Often during the development of a product, features which were initially considered are removed from the scope, or existing code sets (such as 3rd party libraries or open source code) are used to speed up development. However, the more code that exists in a product, the more chances there are for that code to have bugs which can be exploited. Therefore, it is good security practice to remove unwanted or unnecessary features from code prior to using it in production devices, where these features have been deprecated during the development or where they are provide by default by external code (but can be removed or disabled if unwanted). This should be done at the source code level, to ensure that there is the smallest ‘attack surface’ possible in the shipped code files.</p> <p>[UL] 7.5 All protocols present in the device must be documented and justified</p> <p>The security posture of a system is often described as its ‘attack surface’ — the amount of code that can be interacted with is generally directly related to the potential vulnerabilities a system may have. The more code, the more potential vulnerabilities. However, access to this code is of course also important, and the interfaces of a device are the ‘front line’ of the device security, and by definition attacks on devices generally start with these interfaces. Indeed, any device can be summarized by the totality of its inputs, outputs, and internal processing (where the inputs and outputs are the interfaces).</p> <p>Therefore, it is important for all interfaces of the devices to be clearly understood and justified as to their purpose, as an unnecessary interface may be the one that is used to compromise the system. This list of interfaces must include both physical ports (USB, serial, Ethernet, etc) and protocols which are supported on these interfaces. However, this requirement is designed to cover only physical and output-originating protocols — listening services that actively wait for connections over switched and wireless interfaces are covered under a separate requirement below.</p> <p>It is recognized that documenting all protocols supported can be quite complex; for example a USB interface may support many different protocols, classes, and types of devices. However, the goal is to ensure that the totality of the interfaces is well understood and so this exercise is an important one.</p> <p>[UL] 7.6 All services present in the device must be documented and justified</p> <p>For the purposes of this standard a service is considered a super-set of a protocol, in that it actively ‘listens’ for connections across switched or wireless connections. Direct physical interfaces, such as serial or JTAG, are generally considered not to be a ‘service’.</p> <p>As with protocols, listening services are often the first point of attack on a device, and therefore can be the first line of defense to prevent such attacks. Justification of enabled services is vital to understand the security posture of the system, and ensure that sufficient security measures are put in place to protect these interfaces.</p> <p>It is understood that additional services may be included in a device as a product differentiator, or to provide value-added services to specific market segments. It is recommended that consideration be given to limiting the functionality of the system ‘out of the box’ and instead providing options for users to enable features where they see a need.</p>
Additional IoT Device Security Capabilities and Practices	Physical Access Control	



CATEGORY	SUB-CATEGORY	MAPS TO
Additional IoT Device Security Capabilities and Practices	Best Practices	<p>[UL] 6.5 Switched or wireless connections must allow for the use of an industry standard security protocol (such as TLS)</p> <p>A formal security protocol is essential when communicating over remote or wireless connections. It is a requirement that systems allow for the use of an industry standard ‘best practice’ public protocol (such as TLS). , A proprietary protocol that has been designed with the light weight needs of the IoT space in mind may also be implemented, but customers must be provided with the ability to choose which protocol they wish to use, and any proprietary protocols implemented may require the device to undergo more detailed testing. It should be noted that this requirement does not mandate that all communications must be performed using this protocol — for example, a light bulb may allow for the changing of brightness without implementing encryption of the command — but the protocol must be available for use, and must always be used for any security sensitive communications.</p> <p>[UL] 6.4 Security protocols must implement secure defaults, and prevent downgrade attacks</p> <p>Many security protocols, such as TLS, allow for the use of insecure protocols and methods. Even when secure options are used, sometimes the connection can be forced to downgrade to a less secure option if it is not correctly configured.</p> <p>[UL] 6.2 Device must support industry accepted wireless security defaults for any Wi-Fi connections</p> <p>Where devices implement Wi-Fi connections, it is important that these devices do not force a reduction in the security of the customers Wi-Fi implementation. For example, a poorly designed system may force the customer to change from WPA2 security to using WEP, which is considered insecure.</p>



## 21 | Sponsoring Organizations

**About CSDE** ▶ The Council to Secure the Digital Economy (CSDE) brings together companies from across the information and communications technology (ICT) sector to combat increasingly sophisticated and emerging cyber threats through collaborative actions. Members include Akamai, AT&T, CA Technologies, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefonica and Verizon. CSDE is coordinated by USTelecom and the Consumer Technology Association.

**About USTelecom** ▶ USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives— all providing advanced communications service to both urban and rural markets.

**About the Consumer Technology Association** ▶ The Consumer Technology Association (CTA)<sup>™</sup> is the trade association representing the \$377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies — 80 percent are small businesses and startups; others are among the world's best-known brands — enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES<sup>®</sup> — the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

## 22 | Endnotes

- 1 Daniel Newman, *The Top 8 IoT Trends for 2018*, Forbes (Dec. 19, 2017), <https://www.forbes.com/sites/danielnewman/2017/12/19/the-top-8-iot-trends-for-2018/#2523096867f7> (citing HIS Markit IoT Trend Watch 2018, available at <https://ihsmarkit.com/industry/telecommunications.html>); See also Gartner, *Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>.
- 2 See, e.g., Catalin Cimpanu, *Sly Malware Author Hides Cryptomining Botnet Behind Ever-shifting Proxy Service*, ZDNet (Sept. 13, 2018), <https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service/> (“[B]otnets focused on cryptocurrency mining operations have been one of the most active forms of malware infections in 2018.”)
- 3 Sam Thielman and Chris Johnston, *Major Cyber Attack Disrupts Internet Service Across Europe and US*, The Guardian, (Oct. 21, 2016), <https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service>.
- 4 Michael Newberg, *As Many as 48 Million Twitter Accounts Aren’t People, Says Study*, CNBC (Mar. 10, 2017), <https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html>.
- 5 JP Buntinx, *Top 4 Largest Botnets to Date*, Null TX (Jan. 7, 2017).
- 6 <https://www.csis.org/analysis/extending-federal-cybersecurity-endpoint>
- 7 <https://www.catonetworks.com/blog/iot-security-standards-and-initiatives/>
- 8 European Commission, *EU negotiators agree on strengthening Europe’s cybersecurity*, Dec. 2018, [http://europa.eu/rapid/press-release\\_IP-18-6759\\_en.htm](http://europa.eu/rapid/press-release_IP-18-6759_en.htm)
- 9 Japan Ministry of Economy, Trade and Industry, *METI Compiles Results of the Call for Public Comments on the Draft Cyber/Physical Security Framework*, [https://www.meti.go.jp/english/press/2018/1001\\_002.html](https://www.meti.go.jp/english/press/2018/1001_002.html)
- 10 UK Department of Digital, Culture, Media & Sport, *Code of Practice for Consumer IoT Security*, Oct. 2018, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/773867/Code\\_of\\_Practice\\_for\\_Consumer\\_IoT\\_Security\\_October\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf)
- 11 UK Department of Digital, Culture, Media & Sport, *Consultation on regulatory proposals on consumer IoT security*, <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>, May 2019
- 12 NIST, *NIST Cybersecurity for IoT Program*, retrieved Mar. 2019, <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>
- 13 E.g., <https://www.publicknowledge.org/press-release/new-public-knowledge-paper-proposes-security-shield-label-to-support-sustainable-cybersecurity>.
- 14 See the informative references section for industry voluntary consensus standards and best practices.
- 15 Available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf>. Further work is available at [https://www.nist.gov/sites/default/files/documents/2019/02/01/final\\_core\\_iiot\\_cybersecurity\\_capabilities\\_baseline\\_considerations.pdf](https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iiot_cybersecurity_capabilities_baseline_considerations.pdf).
- 16 Available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf>.
- 17 See Rob van der Meulen, *Gartner Says 8.4 Billion “Things” Will Be in Use in 2017, Up 31 Percent From 2016*, Gartner (Feb. 7, 2017), <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016> (reporting that the majority of the IoT market is comprised of consumer applications, which are generally less complex devices).
- 18 Or software-hardware hybrid.
- 19 In this case, a user may refer to the consumer using a device, a technician responsible for installation or maintenance, an authorized employee in a managed environment, etc.
- 20 Transport Layer Security version 1.3, see <https://datatracker.ietf.org/doc/rfc8446/>.
- 21 *Prohibiting Secure Sockets Layer (SSL) Version 2.0*, see <https://tools.ietf.org/html/rfc6176>.
- 22 See, e.g., [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- 23 Updateability may also be referred to as agility.
- 24 For more information on coordinated vulnerability disclosure, see *The CERT Guide to Coordinated Vulnerability Disclosure*, <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330>. ISO 30111 (internal processes) and ISO 29147 (disclosure) are good references as well on this topic, as well as Center for Cybersecurity Policy and Law’s *Improving Hardware Component Vulnerability Disclosure*, <https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure>.
- 25 See <https://datatracker.ietf.org/doc/rfc8520/>
- 26 OMA Device Management, see [http://www.openmobilealliance.org/wp/overviews/dm\\_overview.html](http://www.openmobilealliance.org/wp/overviews/dm_overview.html)
- 27 See <https://www.broadband-forum.org/download/TR-069.pdf>
- 28 IoTSense: Behavioral Fingerprinting of IoT Devices, Colorado State University, April 2018, <https://arxiv.org/pdf/1804.03852.pdf>
- 29 For example, <https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/iiot-ddos-project-description-final.pdf>
- 30 See also <https://github.com/w3c/wot-security-testing-plan> for an open-source IoT security testing plan, including functional and adversarial testing, and a security test plan framework.
- 31 See also <https://www.ul.com/resources/ul-cybersecurity-assurance-program-ul-cap> for the UL Cybersecurity Assurance Program.
- 32 NIST, essay referenced in blog post Let’s talk about IoT device security, Feb. 2019, [https://www.nist.gov/sites/default/files/documents/2019/02/01/final\\_core\\_iiot\\_cybersecurity\\_capabilities\\_baseline\\_considerations.pdf](https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iiot_cybersecurity_capabilities_baseline_considerations.pdf)
- 33 Ibid.
- 34 See *EU Agency for Cybersecurity Baseline Security Recommendations for IoT*, <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iiot>



